PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR – MATRIZ

FACULTAD DE CIENCIAS ADMINISTRATIVAS Y CONTABLES

TESIS DE MAGÍSTER EN ADMINISTRACIÓN DE EMPRESAS CON MENCIÓN EN GERENCIA DE LA CALIDAD Y PRODUCTIVIDAD

METODOLOGÍA DE IMPLEMENTACIÓN DE UNA CULTURA ORGANIZACIONAL BASADA EN EL SISTEMA COSO -ERM PARA LA UNIDAD DE AUDITORÍA INTERNA EN UNA INSTITUCIÓN FINANCIERA EN QUITO

ING. ANDREA CECILIA CUADRADO TAPIA

DIRECTOR: ING. VÍCTOR HUGO RAMÍREZ LAFUENTE, MBA.

QUITO, 2014

DIRECTOR DE TESIS

Ing. Víctor Hugo Ramírez Lafuente, MBA.

INFORMANTES

Ing. Rodrigo Saltos Mosquera, MBA.

Ing. Álvaro Burgos Yánez, MSc.

DEDICATORIA

Dedico este trabajo de investigación con todo mi amor a mis padres, hermanas y sobrinas que hicieron y me dieron todo en la vida para que yo pudiera hoy cumplir otro de mis sueños y objetivos, a mi amado esposo por su apoyo incondicional y paciencia en los días largos durante el desarrollo de este proceso y al resto de mi familia y amigos quienes con su colaboración y confianza han sido partícipes de esta etapa de mi vida. Hoy quiero que ellos sean parte de este triunfo

AGRADECIMIENTO

Agradezco a Dios, por haberme dado la oportunidad de enfrentar, aprender y disfrutar cada reto de mi vida.

A mi esposo, padres, hermanas, cuñados y sobrinas por ser los pilares más fuertes de mi vida, y porque con su apoyo diario son quienes me han motivado a seguir luchando por la consecución de mis ideales, y logro de mis metas.

A la Pontificia Universidad Católica del Ecuador por toda la enseñanza recibida, especialmente al: Ing. Victor Hugo Ramírez, MBA.; Ing. Rodrigo Saltos, MBA.; e Ing. Álvaro Burgos MBA.; por su valioso aporte en este trabajo de investigación.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN EJECUTIVO

La crisis cambió dramáticamente la actitud y el enfoque de las Instituciones Financieras hacia el riesgo muchas de las entidades han adoptado o están adoptando un enfoque más integral, que requiere la implantación de una cultura que genere conciencia sobre la responsabilidad en la identificación del riesgo, de todos los niveles, independientemente de su jerarquía. Las posibilidades de incremento de riesgo y error en el procesamiento dependen en gran medida de la complejidad de las operaciones. Los factores que inciden en la complejidad, entre las más importantes, son: el número de subprocesos que abarca; la participación de varias áreas, número de personas que intervienen; organizaciones de servicio (proveedores externos): tiempo de respuesta para cumplir un ciclo completo, (eficiencia del proceso); y, complejidad tecnológica requerida; y, eficiencia del personal en la ejecución de sus funciones.

Fue necesario revisar el COSO ERM como marco de referencia en la aplicación de la Auditoría Basada en Riesgos, y así establecer lineamientos en los cuales deben enfocarse las revisiones de auditoría, la misma que inicia con una adecuada planificación.

Esta información permitió presentar una metodología para aplicarse en el área de Auditoría Interna y así poder realizar una adecuada planificación de los procesos, tomando en cuenta su nivel de riesgo (alto, moderado y bajo) permitiendo conocer la periodicidad de que procesos se deben priorizar en las revisiones anuales.

Por último, se presenta una Matriz de Factores de Riesgo como parte importante de la metodología de tal manera que su implementación se convierta en una cultura organizacional teniendo como eje principal el Control Interno y la minimización de riesgos, y esta metodología se puede manejar como herramienta de gestión que permita identificar y controlar los riesgos.

INTRODUCCIÓN

El objetivo de esta investigación es desarrollar una metodología de implementación de una cultura organizacional basada en el sistema COSO-ERM para la Unidad de Auditoría Interna de una Institución Financiera de Quito

Es necesario también, presentar los siguientes objetivos específicos:

- Identificar que es el control Interno, el sistema Coso y Coso-Erm y su aplicabilidad en una Institución Financiera.
- Analizar la gestión de Riesgos como tema relacionado en el desempeño de una Unidad de Auditoría Interna en una Institución Financiera.
- Determinar los beneficios y /o consecuencias de aplicar una Metodología de valoración de procesos en función de factores de riesgo en la Unidad de Auditoría Interna en una institución Financiera de Quito
- Establecer propuestas de solución a los puntos débiles presentados en la aplicación de la metodología en la Unidad de Auditoría Interna en una institución Financiera de Quito

Para conseguirlo, se realiza un estudio de los aspectos generales que encierran al Control Interno y su evolución, sus modelos de controles como el Sistema COSO sus componentes, el marco metodológico de la gestión de riesgos de las empresas del Ecuador y su influencia principalmente en la Banca y Finanzas a través de comparaciones y estadísticas de los top 10 de riesgos en las industrias y la Banca presentados por una de la firmas consultoras del país E&Y. Se amplía la información del COSO ERM y su aplicación se describe su estructura sus componentes sus beneficios y limitaciones, se indica lo que implica un riesgo empresarial y los controles a implementarse con una adecuada administración de riesgos.

También se describe aspectos generales de la Cultura Organizacional como un proceso importante del cambio de visión y aplicación en la Institución Financiera, tipos de cultura aplicables al desarrollo dentro de una organización.

Así mismo es importante conocer el enfoque de la Auditoría Interna y la Gestión de Riesgos, por ellos en el capítulo dos se indica sus enfoques tradicionales con los nuevos tratando de obtener una calidad total y mejoramiento continuo.
Para ello es importante conocer los lineamientos que describe el Instituto de Auditores Internos con relación a la Gestión de Riesgos de la empresa, sus posiciones frente al tema y los roles fundamentales, tomando en cuenta el rol de la auditor interno en este tema

Así mismo es importante conocer lo que indica el ente de control regulador de las Instituciones del Sistema Financiero, describiendo lo que indica la Resolución de la Junta Bancaria No. JB-2010-1549, del 21 de enero de 2010 que plasma lineamientos sobre la Auditoría Interna y su gestión con los riesgos, se analiza a detalle el enfoque de la Auditoría Basada en Riesgos., y su aplicación se indica las normas y las buenas practicas relacionadas que rigen para todas las unidades de auditoría por el I.A.I. Se finaliza con un diagnóstico las fortalezas, debilidades, oportunidades y amenazas que afectan a la Institución y que pueden ser eje principal para desarrollar una metodología que enfoque la prevención de riesgos.

En un tercer capítulo se desarrolla en base a toda la investigación la metodología de valoración de procesos en función de los factores de riesgos, se toma como referencia lo que indica el I.A.I. en base al COSO ERM, se diseña una metodología con procedimientos y actividades a seguir, se describe cada actividad, como se debe elaborar y las fuentes de información que deben ser obtenidas para ser sujetas al desarrollo de este proceso, se crea los formatos clave para la consecución de la metodología y como principal y relevante actividad es la elaboración de la Matriz de Factores de Riesgo de Auditoría que fue desarrollada en base a los principales riesgos críticos que la Institución mantiene y a los riesgos inherentes y de control a los cuales se enfrentan los procesos, desarrollando factores de riesgos.
En todas las empresas existen riesgos, pero algunos imposibles de eliminar; sin embargo, el panorama de factores de riesgo permite identificarlos y visualizar de forma general como se encuentra el proceso y en algunos casos estos factores ayudan a determinar ciertas debilidades de control interno y las acciones que se pueden implementar para mitigarlos. Con el objeto de limitar la existencia de subjetividad en la evaluación, soportar y facilitar el análisis de los factores de riesgo, estos fueron ampliados en sub factores, en los cuales, cada uno de ellos

incluye criterios de evaluación. Los factores de riesgo están relacionados generalmente con el alcance de las actividades de control diseñadas en los procesos con el propósito de asegurar que se logre sus objetivos, con el apoyo del personal que participa en el desarrollo de las actividades y la gestión del proceso y el entorno y naturaleza en el que este funciona.

Una vez diseñada la matriz de factores de riesgo, se debe calificar los procesos que forman parte del Universo Auditable conforme la Matriz, en función de la calificación obtenida se debe determinar los ciclos de revisión: Riesgo Alto se debe revisar cada año, los procesos con riesgo Moderado cada dos años y los procesos con riesgo Bajo cada tres años. Concluyendo con la realización de la planificación anual de la Unidad de Auditoría Interna.

Finalmente, las conclusiones, recomendaciones y propuestas de solución son desarrolladas en el cuarto capítulo.

1. ASPECTOS GENERALES

Para entender lo que es el Control Interno, es necesario estudiar sus antecedentes y metodologías que influyen en su actuar, y su constante evolución, la cual es importante conocer, por otro lado, está la Ley del Sistema Financiero, que pretende impulsar la conciencia de la calidad y la eliminación de riesgos en todo ámbito, así mismo, esta ley contempla el control de estas Instituciones del Sistema Financiero, y finalmente se debe realizar un diagnóstico focalizado en factores políticos, económicos, sociales y tecnológicos

1.1. Antecedentes: Metodologías de Control Interno (Sistema COSO)

Las definiciones sobre el control interno y su función así como las metodologías de evaluación de la eficacia del sistema de control interno han sido muy extensas y variadas. Posiblemente, el primer cambio significativo en la forma de observar el control interno nació a raíz de la necesidad de contar con información fiable. Desde el punto de vista de la auditoría de estados financieros, se ha reconocido hace tiempo que dichos exámenes se pueden ejecutar en forma más eficiente apoyándose en una evaluación del sistema de control interno.

1.1.1. Evolución del Control Interno

Muchas veces las personas que toman decisiones no disponen de la información exacta sobre la consecuencia de sus acciones. En general esto sucede en todo orden de la vida por lo cual no es difícil aceptarlo para el mundo de los negocios en particular. Quien tiene la responsabilidad de tomar una decisión, a la hora de hacerlo, no debe dejar de lado la incertidumbre, cada acción puede conducir a varios resultados posibles, ignorándose cuál de ellos se concretará en la realidad.

La existencia de la incertidumbre aumenta la complejidad del problema, los hombres de negocios buscan permanentemente formas de mejorar sus habilidades en la toma de

decisiones. La búsqueda de la eficiencia, productividad, competitividad y los procesos de globalización han incrementado la importancia de la evaluación adecuadas de riesgos, oportunidades, fortalezas, amenazas y debilidades tendrá mayores resultados en la rentabilidad futura y en la confiabilidad que pueda transmitir a los accionistas y/o interesados.

Desde que existe actividad económica, se han establecido controles para segurar la consecución de los objetivos organizacionales. A lo largo del tiempo el control interno ha sido más significativo para quienes dirigen actividades comerciales, industriales, políticas, estatales, en general cualquier organización orientada a la consecución de determinados objetivos.

Al principio, cuando el comercio era desarrollado por pequeños empresarios, el control interno existía para prevenir fraudes o errores por parte del personal. Las organizaciones buscaban proteger su patrimonio sin importar en mayor medida la eficiencia, surgía para cubrir una necesidad del mercado producto de la visión de algún empresario. En ese contexto no existía un análisis previo sobre la viabilidad del negocio, no existía lo que hoy en día juega un papel primordial en dicho proceso, la planificación estratégica. La contabilidad era muy rudimentaria, cumplía un mero rol de registro y no desempeñaba un papel fundamental en la toma de decisiones.

Desde la década de los cuarenta, las organizaciones profesionales de auditoría interna y externa han realizado publicaciones con recomendaciones y normas sobre la importancia del control interno en las auditorías de los estados financieros.

Actualmente se ha dado mucha importancia al sistema de control interno, tanto entidades del sector público como privado están pendientes del tema. Es en este contexto que los controles internos promueven la eficiencia, reducen los riesgos de pérdida de activos, ayudan asegurar la confiabilidad de la información contable, el cumplimiento de leyes y reglamentaciones.

Las profundas crisis que han atravesado muchos países en la década de los 90s han estimulado la necesidad de fortalecer la estructura del sistema financiero internacional. Esto ha dado lugar a ciertas normas internacionales de supervisión de entidades financieras y de mercado de capitales, destinados a revisar la estabilidad del sistema. Existen diferentes organismos internacionales encargados de la elaboración de dichos estándares.

En general, las organizaciones buscan mayor transparencia en la elaboración de estados contables a través de mejores medidas de control para evitar fraudes financieros de la magnitud de Enron, WorldCom. De esta forma se establecieron mecanismos para asegurar la veracidad y confiabilidad de la información presentada en los estados contables a través de personas independientes de la sociedad y sus miembros. En caso de la industria bancaria, los colapsos financieros hacen necesaria la implantación y mantención de un sólido sistema de control interno.

El informe COSO ha influenciado las leyes y reglamentaciones de muchos países con motivo de los colapsos bancarios y bancarrota de organizaciones en todo el mundo. Por ejemplo, en Uruguay en primera instancia comenzó a tener relevancia para las Empresas de Intermediación Financiera.

En el 2004 se publica la "Administración del Riesgo Empresarial- Marco Integrado (Coso/ERM)". El riesgo se ve como una oportunidad de alcanzar las metas, por tanto las organizaciones deben aprender a administrar el riesgo para transformar las amenazas en nuevas oportunidades que generen mayor valor para los accionistas y/o interesados.

Muchas veces el control interno se utiliza para enunciar las directrices de los dueños, propietarios para dirigir, coordinar y controlar a sus empleados. Edgar Deming (1989), reconocido como el padre del control de la calidad, ha expuesto en sus investigaciones que a mayor calidad menores costos. La Gerencia debe reconocer en todo momento la labor de los empleados y el papel que desempeñan ambos en el control de calidad de la organización.

A lo largo de los años se ha definido al control interno de diferentes formas, tal vez, la definición que más ha predominado entre la literatura, normas y reglamentos puede ser la emitida por el Comité de Auditoría del AICPA (American Institute of Certified Public Accountants), organismo que reúne a los contadores públicos y emite normas para la estandarización del trabajo de los contadores.

1.1.2. Definición del Control Interno:

El control interno son procedimientos implementados por la administración, que deben ser aplicadas por el recurso humano adecuado en cada una de las labores asignadas en una organización para prevenir riesgos de perdida, contribuye también a lograr la eficiencia en cada uno de los procesos y alcanzar los objetivos de la entidad.

- El control interno es un proceso, es decir un medio para alcanzar un fin y no un fin en sí mismo.
- Lo llevan a cabo las personas que actúan en todos los niveles, no se trata solamente de manuales de organización y procedimientos.

El control interno puede ayudar a que la organización consiga sus objetivos de rentabilidad, rendimiento y prevenir la pérdida de recursos.

Ayuda a la obtención de información financiera confiable; a reforzar la confianza en que la organización cumple con las leyes y normas aplicables; y, evitar efectos perjudiciales para su reputación y otras consecuencias.

En resumen, puede ayudar a que la organización llegue a donde quiere ir y evite peligros y sorpresas en el camino.

La principal limitación del control interno es que no garantiza el éxito de una organización, por muy bueno que sea su diseño y funcionamiento, solo proporciona *una "seguridad razonable",* es decir, asegura la consecución de los objetivos básicos empresariales o como mínimo la supervivencia de la organización

1.1.3. Los modelos de los controles actuales:

A partir de la divulgación del informe COSO se han publicado diversos modelos de control, así como numerosos lineamientos para un mejor gobierno corporativo; los más conocidos, además del COSO (USA) son los siguientes:

- Criteria of Control (COCO), del Instituto Canadiense de Contadores Certificados (CICA de las siglas del inglés);
- Cadbury del Instituto de Contadores del Reino Unido;
- King del Instituto de Contadores de Sud-áfrica;
- Vienot de Francia;

Adicionalmente existen regionalmente estos documentos:

- MICIL - Marco Integrado de Control Interno para Latino América (síntesis y adaptación de COSO I).
- CORRE – Control de los Recursos y los Riesgos en Ecuador (síntesis de: COSO I, COSO II (ERM), MICIL).

Según el Informe COSO se define: Control Interno, Componentes y Eficacia

•C- comitte (comité)

•O- of (de)

•S- sponsorig (auspiciantes)

•O- organizations (organizaciones)

Debido a una serie de problemas identificados en el Gobierno de los Estados Unidos de América, en la década de los 70 y llegando a las dificultades financieras del Sistema de Ahorro y Crédito en la década de los 80, la Comisión del Senado de los EUA, Treadway Comission gestionó la formación del Commitee of Sponsoring Organizations (Comité de Organizaciones Patrocinadoras), conocido por sus siglas en inglés, COSO. Este Comité realizó una investigación sobre el conocimiento, aplicación y mejora de los criterios de control interno en las grandes corporaciones, las medianas y pequeñas empresas,

incluyendo temas relacionados con el mejoramiento técnico y el alcance de las funciones de diseño, implantación y evaluación de los controles internos integrados de las organizaciones.

En septiembre de 1992 se publicó la versión en inglés denominado Informe COSO contó con la asistencia técnica permanente de la firma Coopers & Lybrand para la investigación. La traducción del Informe COSO fue realizada por la firma Coopers & Lybrand y el Instituto de Auditores Internos, Capítulo España, y fue publicada en1997.

COSO : Organización voluntaria del sector privado, establecida en los EEUU, dedicada a proporcionar orientación a la gestión ejecutiva y las entidades de gobierno sobre los aspectos fundamentales de organización de este, la ética empresarial, control interno, gestión del riesgo empresarial, el fraude, y la presentación de informes financieros.
COSO ha establecido un modelo común de control interno contra el cual las empresas y organizaciones pueden evaluar sus sistemas de control (Berbia, 2008).

Miembros:

COSO estuvo y está conformado por organismos de profesionales de los Estados Unidos de América (EUA); inició la investigación en 1986, sus miembros son:

1. American Accounting Association (AAA),
2. American Institute of Certified Public Accountants (AICPA),
3. Financial Executive Institute (FEI),
4. Institute of Internal Auditors (IIA) y el
5. Institute of Management Accountants (IMA).

A partir de la publicación del informe COSO (Control Interno- Estructura Integrada) en septiembre del 1992 y en cuyo desarrollo participaron representantes de organizaciones profesionales de contadores de ejecutivos de finanzas y de Auditores Internos, ha resurgido en forma impresionante la atención hacia el mejoramiento del control interno y un mejor gobierno corporativo, lo cual fue derivado de la presión pública para un mejor manejo de

recursos públicos o privados en cualquier tipo de organización. En este sentido conviene recordar que un eficiente sistema de control puede proporcionar un importante factor de tranquilidad, en relación con la responsabilidad de los directivos, los propietarios, los accionistas y los terceros interesados.

1.1.4. Control Interno según COSO:

El control interno se define como un proceso, efectuado por el consejo de administración, la dirección y el resto de personal de una entidad (todos), diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías (Internos, 1997):

1. Eficacia y eficiencia en las operaciones (OPERACIONES).
2. Información financiera confiable (REPORTES FINANCIEROS).
3. Cumplimiento de las leyes y normas aplicables (CUMPLIMIENTO).

"El control interno comprende el plan de organización y todos los métodos y medidas coordinados que se adoptan en un negocio para salvaguardar sus activos, verificar la exactitud la confiabilidad de sus datos contables promover la eficiencia operacional y fomentar la adherencia a las políticas prescritas". (Mantilla & Cante, 2005)

"El control interno es una expresión utilizada para describir todas las medidas tomadas por los propietarios y directores de empresas para dirigir y controlar a los empleados". (Mautz, 1970), establecen que la ley de prácticas corruptas del exterior hace responsable a la gerencia la tenencia de un control interno confiable. Sin embargo, a menos que estén bien definidos, los límites de la responsabilidad gerencial permanecen indeterminados.

"El control interno es el conjunto de reglas, principios o medidas enlazadas entre sí, desarrolladas dentro de una organización, con procedimientos que garanticen su estructura, un esquema humano adecuado a las labores asignadas y al cumplimiento de los planes de acción, con el objeto de lograr: razonable protección del patrimonio, cumplimiento de

políticas prescritas por la organización, información confiable y eficiencia operativa" (SAS 1, 1972)

El control interno es un proceso:
Es un medio utilizado para la consecución de un fin, no un fin en sí mismo. Por ejemplo, un adecuado sistema de control interno fortalece a la organización para la consecución de sus objetivos institucionales, pero no garantiza el cumplimiento de los mismos.

El control interno lo llevan a cabo las personas:
No se trata solamente de manuales de políticas, sino de personas en cada nivel de la organización.

El control interno sólo puede aportar un grado de seguridad razonable:
El Control Interno logra una seguridad razonable y no la seguridad total, en la administración y consecución de los objetivos de la dirección de la organización, ya que ningún control interno es perfecto e infalible.

El control interno está pensado para facilitar la consecución de objetivos:
En una o más de las diferentes actividades de la organización, a través de la interacción de cada uno de los componentes del control interno que, al mismo tiempo, se interrelacionan e interactúan en forma conjunta.

Por ser el modelo mayoritariamente adoptado a la fecha, como referencia tomamos la definición que establece el informe COSO, lo cual señala:

1.1.5. Componentes del Control Interno COSO:

Toda organización, independientemente de la actividad o del sector al que pertenezca, requiere definir y desarrollar los siguientes componentes en el marco integrado de control interno:

1. Ambiente de Control (y Trabajo),
2. Evaluación de Riesgos,
3. Actividades de Control,
4. Información y Comunicación (Sistemas de); y,
5. Supervisión (Monitoreo).

Figura 1, Componentes del Control Interno
Fuente: (Badillo, 2010)

1. <u>Ambiente de control:</u>

Constituye el núcleo de una organización, se refiere a su personal (atributos individuales, incluyendo la integridad, los valores éticos y la profesionalidad) y el entorno en el que trabaja. Los empleados son el motor que impulsa la entidad y los "**cimientos**" sobre los que descansa todo.

2. <u>Evaluación de riesgos:</u>

El segundo componente del control, involucra la identificación y análisis de riesgos relevantes para el logro de los objetivos y la base para determinar la forma en que tales riesgos deben ser manejados. Asimismo se refiere a los mecanismos necesarios para

identificar y manejar riesgos específicos asociados con los cambios, tanto los que influyen en el entorno de la Organización como en el interior de la misma.

3. **Actividades de Control:**

Las actividades de control son aquellas que realizan la Gerencia y demás personal de la Organización para cumplir diariamente con actividades asignadas y ayudan a conseguir una **seguridad razonable** de que se llevan a cabo de forma eficaz las acciones necesarias para afrontar los "**riesgos** "que existen con respecto a la consecución de los **objetivos de la entidad**. Estas actividades están relacionadas (contenidas) con los manuales, políticas, sistemas y procedimientos principalmente.

4. **Información y Comunicación:**

Así como es necesario que todo el personal conozca el papel que les corresponde desempeñar en la organización (funciones y responsabilidades), es imprescindible que cuenten con los sistemas que proporcionen la información periódica y una comunicación oportuna para orientar las acciones del personal en consonancia con los demás, hacia el mejor logro de los objetivos. Esto permite que el personal capte e intercambie la información requerida para desarrollar, gestionar y controlar sus operaciones.

5. **Supervisión o Monitoreo**

En general los sistemas de control están diseñados para operar en determinadas circunstancias; sin embargo, las condiciones evolucionan debido tanto a factores externos como internos colocando con ello que los controles pierdan su eficiencia.
Como resultado de todo ello, la Gerencia debe llevar a cabo la revisión y evaluación sistemática de los componentes y elementos que forman parte de los sistemas de control interno, de esta manera el sistema puede "reaccionar" y "cambiar" de acuerdo a las circunstancias.

1.1.6. Eficacia del COSO:

Los sistemas de control interno de las diferentes organizaciones funcionan a distintos niveles de eficacia. De la misma forma, un sistema determinado puede funcionar de forma diferente en momentos distintos. Cuando un sistema de control interno alcanza el estándar descrito a continuación puede considerarse un sistema eficaz.

El control interno puede considerarse eficaz en cada una de las tres categorías, si el Consejo de Administración y la Dirección tienen una seguridad razonable de que:

1. Disponen de información adecuada sobre hasta qué punto se están logrando los objetivos operacionales de la organización.
2. Se preparan de forma fiable los estados financieros
3. Se cumple las normas y leyes aplicables

1.1.7. Marco Integrado de Control (Framework)

El MICIL incluye los cinco componentes de control interno que constituyen la base para construir la pirámide con similares contenidos, en una demostración de la solidez del control interno institucional para el funcionamiento participativo, organizado, sistematizado, disciplinado y sensibilizado (empoderamiento) del recurso humano para el logro de los objetivos de la organización. Los cinco componentes incorporados en la pirámide de control interno permiten observar de manera objetiva la relación existente entre cada uno de ellos, cuando el segmento asignado a cada uno se junta con otro u otros componentes y la manera como la debilidad o la ausencia de uno de ellos, promueve el desarrollo o facilita el deterioro del conjunto. Los componentes de control interno presentan un esquema que partiendo del ambiente de control como la parte más amplia de la pirámide auspicia el funcionamiento efectivo de los cuatro componentes (evaluación de riesgo, actividades de control, información y comunicación y supervisión) que se asientan sobre él, llegan hasta el final y asegurando su funcionamiento en todos los niveles de la organización. El componente información y comunicación es el más dinámico y permite su

interrelación desde la base de la pirámide (ambiente de control) hasta la cúspide (supervisión). Mediante los reportes procesados para los diferentes niveles y en varias instancias; regresa a la base de la pirámide a través de la comunicación que se procesa desde la supervisión hacia los tres componentes y así completar el proceso a llegar a la base de pirámide.

1.1.8. Control Interno Tradicional – Moderno (COSO)

Dentro de los objetivos de control interno se destacan (Berbia, 2008):

OBJETIVOS DEL CONTROL INTERNO (DIFERENCIAS)	
"Enfoque tradicional"	**Enfoque "Moderno (COSO)"**
La salvaguarda de los activos	**Eficacia y eficiencia de las Operaciones**
La información exacta, confiable y oportuna	**Confiabilidad de la información financiera**
La eficiencia operativa	**Cumplimiento de leyes y regulaciones**
La adhesión a las políticas de la organización	
ELEMENTOS DEL CONTROL INTERNO (DIFERENCIAS)	
"Enfoque tradicional"	**Enfoque "Moderno (COSO)"**
Un plan de organización adecuado	**Ambiente o Entorno de Control**
Un sistema de autorización y procedimientos	**Evaluación de Riesgos**
Personal adecuado	**Actividades de Control**
Prácticas sanas	**Información y Comunicación**
	Supervisión

Figura 2, Objetivos del Control Interno Enfoque Tradicional y Moderno
Fuente: (Berbia, 2008)

1.2. Marco Metodológico de Gestión de Riesgos (Sistema COSO ERM)

A continuación se lista los principales marcos metodológicos sobre gestión de riesgos:

Gestión de riesgos corporativos.

- Estándar ASNZS4360: 1999 de Gestión de Riesgos (Australiano Neozelandés -1999)
- Estándar ASNZS4360: 2004 de Gestión de Riesgos (AustralianoNeozelandés-2004)

- COSO - ERM/Enterprise Risk Management (2004)
- Basilea II – Gestión de Riesgos en Entidades Financieras (2004)
- ISO 31000: 2009 Gestión de Riesgos - Principios y Directrices (2009)
    - ISO73:2009, el vocabulario de gestión de riesgos
    - ISO/IEC 31010: 2009 Risk management –Risk assessment techniques

Gestión de riesgos de Tecnología de la Información TI.

- COBIT - Control Objectives for Information andrelated Technology (ISACA)
- Risk IT (ISACA)
- ISO 27005 Gestión del Riesgo en la Seguridad de la Información
- MAGERIT - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (Gobierno de España)
- OCTAVE – Operational Critical Threat, Assetand Vulnerability Evaluation – Evaluación de Amenazas y Vulnerabilidades de Recursos Críticos Operacionales (Carnegie Mellon University)
-

En septiembre de 2004 se publicó la versión en inglés del COSO ERM (Enterprise Risk Management – Integrated Framework).

La traducción al español del COSO ERM fue realizada por la firma auditora Price wáter house Coopers PWC y la Federación Latino americana de Auditores Internos FLAI, y fue publicada en diciembre de 2005

1.2.1. Inicio del ERM

ERM comenzó en las empresas de servicios financieros, seguros, servicios públicos, petróleo, gas, e industrias manufactureras químicas. En estas industrias los riesgos están bien documentados y medidos. Comúnmente se utilizan sofisticados modelos estadísticos existe entendimiento y supervisión sobre la sensibilidad del mercado y riesgos.

La premisa subyacente del E.R.M. es que cada entidad existe para proveer valor para sus stakeholders. Todas las entidades enfrentan incertidumbre, y el desafío que enfrenta la administración es determinar qué tanta incertidumbre sea aceptable en su búsqueda de hacer que crezca el valor de stakeholders.

La incertidumbre ofrece tanto riesgos como oportunidades, con el potencial de erosionar o enriquecer el valor. El E.R.M. le permite a la administración tratar de manera efectiva la incertidumbre, los riesgos y las oportunidades, enriqueciendo la capacidad de construir valor.

El valor se maximiza cuando la administración define estrategias y objetivos orientados a conseguir un balance óptimo entre las metas de crecimiento y retorno así como los riesgos relacionados, a la vez que despliega recursos eficiente y efectivamente para el cumplimiento de esos objetivos. La administración de riesgos empresarial E.R.M. comprende:

- **Alinear el apetito por el riesgo y la estrategia:** Al evaluar las alternativas estratégicas, definir los objetivos relacionados, y desarrollar los mecanismos para administrar los riesgos relacionados, la administración considera el apetito que por el riesgo tiene la entidad.

- **Enriquecer las decisiones de respuesta al riesgo:** La administración de riesgos empresarial E.R.M. provee el rigor para identificar y seleccionar entre las alternativas de respuesta al riesgo, evitar, reducir, compartir, y aceptar el riesgo.
- **Reducir sorpresas y pérdidas operacionales:** las entidades consiguen capacidad enriquecida para identificar eventos potenciales y establecer respuestas, reduciendo las sorpresas y los costos o pérdidas asociados con éstas.

- **Identificar y administrar riesgos empresariales múltiples y transversales:** cada riesgo afecta diferentes partes de la administración, y el E.R.M. facilita la respuesta

efectiva a los impactos interrelacionados, así como respuestas integradas frente a riesgos múltiples.

- **Sopesar oportunidades:** Mediante la consideración de un rango pleno de eventos potenciales, la administración está posicionada para identificar y realizar de manera proactiva las oportunidades.

- **Mejorar el despliegue del capital:** La obtención de información robusta sobre el riesgo le permite a la administración valorar de manera efectiva las necesidades de capital y enriquecer la asignación del capital.

Esas capacidades son inherentes al E.R.M. y le ayudan a la administración a lograr los indicadores de desempeño y rentabilidad que tiene la entidad, así como a prevenir la pérdida de recursos. El E.R.M. ayuda a asegurar de manera efectiva la presentación de reportes y el cumplimiento con leyes y regulaciones, y ayuda a evitar el daño a la reputación de la entidad y las consecuencias asociadas a ello. En resumen, el E.R.M. le ayuda a la entidad a ir a dónde quiere ir y a evitar escollos y sorpresas en el camino.

1.2.2. Estructura conceptual del ERM

> "(…) El período de desarrollo de la estructura conceptual estuvo caracterizado por una serie de escándalos y fracasos en negocios de alto perfil en los que inversionistas, personal de la compañía, y otros stakeholders sufrieron tremendas pérdidas. En el período subsiguiente a ellos hubo demandas por gobiernos corporativos y administración de riesgos enriquecidos, con nuevas leyes, regulaciones, y estándares de registro. Se hizo más imperativa la necesidad de una estructura conceptual de administración de riesgos del emprendimiento, que proveyera principios y conceptos clave, un lenguaje común, y dirección y orientación claros. COSO considera que esta Administración de riesgos del emprendimiento estructura conceptual integrada satisface esta necesidad, y espera

que será ampliamente aceptada por compañías y otras organizaciones, así como por todos los stakeholders y partes interesadas.

Esta Administración de riesgos empresariales – Estructura conceptual integrada amplía lo relacionado con el control interno, proveyendo un centro de atención más robusto y extensivo sobre el tema amplio de la administración de riesgos del emprendimiento.

No tiene la intención, y no reemplaza, la estructura conceptual integrada de control interno, sino que la incorpora, de manera que las compañías pueden decidir mirar esta estructura conceptual de administración de riesgos de emprendimiento tanto para satisfacer las necesidades de control interno como para moverse hacia un proceso más pleno de administración de riesgos. (…)" ***John J. Flaherty - Presidente, COSO & Tony Maki – Presidente, COSO Advisory Council.***

Figura 3, Componentes del Coso II ERM

Fuente: (Badillo, 2010)

1.2.3. Definición del COSO ERM

El E.R.M. es un proceso efectuado por la junta de directores de una entidad, por la administración y por otro personal, aplicado en el establecimiento de la estrategia y a través del emprendimiento, diseñado para identificar los eventos potenciales que pueden afectar la entidad, y para administrar los riesgos que se encuentran dentro de su apetito por el riesgo, a fin de proveer seguridad razonable en relación con el logro de los objetivos de la entidad.

En el contexto de la misión o visión establecida de una entidad, la administración establece objetivos estratégicos, selecciona estrategias, y establece objetivos alineados que van en cascada a través de la empresa. Esta estructura conceptual de la administración de riesgos empresariales (E.R.M.), que está enfocada al logro de los objetivos de una entidad, se expresa en cuatro categorías:

1. ESTRATÉGICA. (Metas de alto nivel, alineadas con y apoyando su misión), (esta categoría no incluía COSO I).
2. OPERACIONES. Eficiencia y efectividad de los recursos.
3. REPORTES. Confiabilidad de la presentación de reportes.
4. CUMPLIMIENTO. Cumplimiento con las leyes y regulaciones aplicables.

1.2.4. Componentes del ERM

El ERM consta de ocho componentes interrelacionados. Estos, se derivan de la manera como la administración opera un riesgo empresarial y están integrados dentro del proceso administrativo. Estos componentes son:

1. Ambiente Interno:

- El ambiente interno comprende el tono de una organización sirve como la base fundamental para los otros componentes del ERM, dándole disciplina y estructura.

- Dentro de la empresa sirve para que los empleados creen conciencia de los riesgos que se pueden presentar en la empresa.

2. Establecimiento de Objetivos:

- Es importante para que la empresa prevenga los riesgos, tenga una identificación de los eventos, una evaluación del riesgo y una clara respuesta a los riesgos en la empresa.
- Asegura que la administración tiene en funcionamiento un proceso para establecer objetivos y que los objetivos seleccionados apoyan y están alineados con la misión de la entidad y sin consistentes con su apetito por el riesgo.

3. Identificación de eventos:

- Se debe identificar los eventos que afectan los objetivos de la organización aunque estos sean positivos, negativos o ambos, para que la empresa los pueda enfrentar y proveer de la mejor forma posible.
- La empresa debe identificar los eventos y debe diagnosticarlos como oportunidades o riesgos. Las oportunidades se canalizan hacia la estrategia de la administración o hacia el proceso de establecimiento de objetivos.

4. Valoración del riesgo:

- Los riesgos se analizan, considerando su probabilidad e impacto, como una base para determinar cómo se deben administrar.

5. Respuesta al Riesgo:

- La administración selecciona las respuestas al riesgo en cuatro categorías: evitarlo, reducirlo, compartirlo y aceptarlo.

- Evitarlo: Implica dejar las actividades que generan el riesgo (dejar de elaborar un producto o servicio, dejar un mercado, o vender una división de la empresa.
- Reducirlo: Consiste en implementar acciones para disminuir la probabilidad y/o el impacto del riesgo.
- Compartirlo: Trasladar parte de la probabilidad y/o el impacto del riesgo a otros (seguros, tercerización, franquicias)
- Aceptarlo: Implica no realizar ninguna acción para afectarla probabilidad y/o el impacto del riesgo.

6. Actividades de control:

- Políticas y procedimientos que ayudan a asegurar que las respuestas al riesgo son apropiadamente ejecutada. Ocurre a través de todos los niveles de la organización.

7. Información y comunicación:

- Información pertinente (interna y externa) debe ser identificada, capturada y comunicada en una forma y marco de tiempo que permita al personal llevar a cabo sus responsabilidades.
- La comunicación efectiva puede ocurrir en un sentido amplio, de arriba hacia abajo y viceversa, y a todo nivel de toda la entidad.

8. Monitoreo:

- Todo el proceso debe ser supervisado y las modificaciones deben ser realizadas según se necesiten.
- De esta manera el sistema puede reaccionar dinámicamente, cambiando según las condiciones lo requieran.

1.2.5. Beneficios del ERM

El ERM puede realizar una enorme contribución ayudando a la organización a gestionar los riesgos para poder alcanzar sus objetivos.

- Alinea el apetito de riesgo y la estrategia.
- Relaciona crecimiento, riesgo y retorno.
- Amplía las decisiones de respuesta al riesgo.
- Minimiza sorpresas y pérdidas operacionales.
- Identifica y administra riesgos a lo largo de toda la organización.
- Proporciona respuestas integradas a los múltiples riesgos.
- Toma ventaja de las oportunidades.
- Mejora la distribución de capital. (Badillo, 2010)

1.2.6. Limitaciones del ERM

Algunas limitaciones del control son:

- Criterio.- Tomar malas decisiones (errores de juicio en la toma de decisiones).
- Fracasos.- La gente que tiene la responsabilidad de la gestión de riesgos puede equivocarse.
- Disfunciones del Sistema.- Errores por mala interpretación, negligencia, distracción, dejadez, fatiga.
- Transgresión Gerencial.- Un gerente puede eludir intencionalmente las prácticas establecidas debido a fines inadecuados (inobservancia gerencial a las políticas o procedimientos prescritos).
- Colusión.- Dos o más personas pueden colaborar para quebrar controles (confabulación).
- Costo - Beneficio. Los recursos son limitados (los gerentes aceptan correctamente un grado de riesgo cuando el costo del control de ese riesgo excede el beneficio). (Badillo, 2010)

Análisis:

COSO "ERM" II toma muchos aspectos importantes que el coso I no considera, como por ejemplo

- El establecimiento de objetivos
- Identificación de riesgo
- Respuesta a los riesgos

Se puede decir que estos componentes son claves para definir las metas de la empresa.
Si los objetivos son claros se puede decidir que riegos tomar para hacer realidad las metas de la organización.

De esta manera se puede hacer una clara identificación, evaluación, mitigación y respuesta para los riesgos. (Auditoría, 2009)

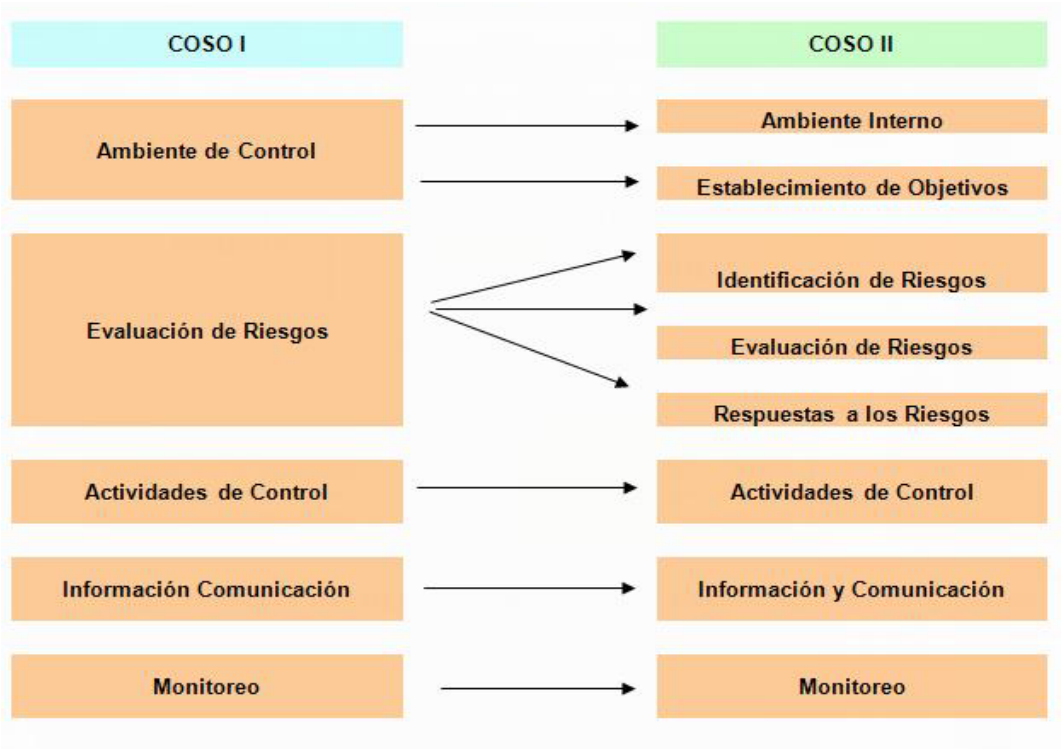


Figura 4, Relación entre Coso I y Coso II
Fuente: (Auditoría, 2009)

1.3. Riesgo y Control

1.3.1. Definición de riesgo:

Riesgo es un término proveniente del italiano, idioma que, a su vez, lo adoptó de una palabra del árabe clásico que podría traducirse como "lo que depara la providencia". El término hace referencia a la proximidad o contingencia de un posible daño. La noción de riesgo suele utilizarse como sinónimo de peligro. El riesgo, sin embargo, está vinculado a la vulnerabilidad, mientras que el peligro aparece asociado a la factibilidad del perjuicio o daño. Es posible distinguir, por lo tanto, entre riesgo (la posibilidad de daño) y peligro (la probabilidad de accidente o patología). En otras palabras, el peligro es una causa del riesgo.
Otro concepto generalmente vinculado al de riesgo es amenaza, y se trata de un dicho o hecho que anticipa un daño. Algo puede ser considerado como una amenaza cuando existe al menos un incidente específico en el cual la amenaza se haya concretado. (WordPress, 2004)

Existen riesgos de distinto tipo y que surgen en diferentes ámbitos. El riesgo laboral, por ejemplo, permite hacer referencia a la falta de estabilidad o seguridad en un trabajo. El riesgo biológico, por otra parte, hace mención a la posibilidad de contagio en medio de una epidemia o por el contacto con materiales biológicos que son potencialmente peligrosos.

El riesgo financiero, por último, está relacionado a la solvencia monetaria de una persona, una empresa o un país. Esta noción se refiere a la capacidad de pago de una deuda contraída. Un país con altos niveles de desocupación, baja producción, elevada inflación y grandes deudas, presenta un riesgo financiero muy alto. Por eso, es poco probable que dicha nación acceda a nuevos créditos, ya que se enfrentaría a serias dificultades para pagarlos. (WordPress, 2004)

Riesgo es la vulnerabilidad ante un potencial perjuicio o daño para las unidades, personas, organizaciones o entidades. Cuanto mayor es la vulnerabilidad mayor es el riesgo, pero

cuanto más factible es el perjuicio o daño, mayor es el peligro. Por tanto, el riesgo se refiere sólo a la teórica "posibilidad de daño" bajo determinadas circunstancias, mientras que el peligro se refiere sólo a la teórica "probabilidad de daño" bajo esas circunstancias.

Por ejemplo, desde el punto de vista del riesgo de daños a la integridad física de las personas, cuanto mayor es la velocidad de circulación de un vehículo en carretera mayor es el "riesgo de daño" para sus ocupantes, mientras que cuanto mayor es la imprudencia al conducir mayor es el "peligro de accidente" (y también es mayor el riesgo del daño consecuente) (Wikipedia)

Toda organización debe hacer frente a una serie de factores internos o externos, que pueden afectar el negocio. El informe COSO define ciertos factores de riesgo externos (cambios tecnológicos, cambios en las expectativas de los clientes, catástrofes naturales, cambios económicos y en las leyes y reglamentaciones) e internos (interrupciones en los sistemas informáticos, deterioro de la calidad del personal contratado, cambio en la asignación de responsabilidades, actividades y accesibilidad a los activos)

Riesgo.- Es la posibilidad de que ocurra un acontecimiento que tenga un impacto en el alcance de los objetivos. El riesgo se mide en términos de consecuencias y probabilidad.

Riesgo Residual.- Son los riesgos que permanecen después de que la Dirección haya realizado sus acciones para reducir el impacto y la probabilidad de un acontecimiento adverso, incluyendo las actividades de control en respuesta de un riesgo.

Interpretación académica.- Es una medida de incertidumbre que involucra el logro de los objetivos institucionales, lo que incluye las consecuencias y probabilidad de que un evento negativo ocurra.

El riesgo es por sí mismo una condición de la existencia, es inherente a cualquier recurso o actividad; por ello el riesgo no se crea ni se destruye; solo se transforma.

Riesgos de Auditoría:

El Riesgo de auditoría es la posibilidad de que la información o actividad sujeta a examen contenga errores o irregularidades significativas y no sean detectados en la ejecución. El riesgo de auditoría está compuesto por:

a) **Riesgo inherente**.- Es la posibilidad de que existan errores o irregularidades en la gestión administrativa y financiera, antes de verificar la eficiencia del control interno diseñado y aplicado por el ente a ser auditado. Este riesgo tiene relación directa con el contexto global de una institución e incluso puede afectar a su gestión.

b) **Riesgo de control.-** Es la posibilidad de que los procedimientos de control interno incluyendo a la unidad de auditoría interna, no puedan prevenir o detectar los errores significativos de manera oportuna. Este riesgo si bien no afecta a la entidad como un todo, incide de manera directa en los componentes.

c) **Riesgo de detección.-** Se origina al aplicar procedimientos que no son suficientes para lograr descubrir errores o irregularidades que sean significativos, es decir, que no detecten una debilidad de control o hallazgo que pudiera ser importante.

1.3.2. Riesgo Empresarial

Se produce riesgo cuando hay probabilidad de que algo negativo suceda o que algo positivo no suceda, la ventaja de una empresa es que conozca claramente los riesgos oportunamente y tenga la capacidad para afrontarlos. El Riesgo es un concepto que bien podríamos llamar vital, por su vínculo con todo lo que hacemos, casi podríamos decir que no hay actividad de la vida, de los negocios o de cualquier asunto que se nos ocurra, que no incluya la palabra riesgo.

Fue por ello que la humanidad, desde sus inicios, buscó maneras de protegerse contra las contingencias del quehacer diario y desarrolló al igual que la mayoría de las especies

animales maneras de esquivar, eliminar, minimizar o enfrentar los riesgos. Entre esas formas de protección está la acción colectiva, cooperada o sindicalizada; la precaución individual o corporativa, las normas comunitarias y en fin tantas otras, entre las cuales se incluye la tecnología como medio de prevención.

Para ello, las empresas están adoptando profesionalmente funciones específicas manejados por departamentos especializados en las identificación del riesgo no solo de sus activos, sino de sus pasivos, equilibrando la rentabilidad y la de poder asumir los riesgos implícitos en los negocios, denominándolas Gerencias de Riesgos, logrando así una mayor eficiencia y eficacia de los procesos para una mayor efectividad y seguridad razonable, como también determinado factores de mecanismos de medición, fuentes de información confiables, oportunas, series históricas de valores relevantes y sistemas computarizados (softwares) de identificación y corrección.

1.3.2.1. Origen de los Riesgos:

Pueden ser derivados por las amenazas externas y las debilidades internas, algunos cuantificables y otros no originados específicamente por inadecuada estructura organizacional, la competencia desleal, por la mala calidad de los productos, por exigencias exageradas de los empleados, huelgas, nuevos impuestos, catástrofes, iliquidez, tasas de interés exageradas, aumento de precios de los proveedores, pérdida de imagen, por inadecuada auditoría externa e interna o por autocontroles no aplicados, etc.
Se pueden clasificar los diferentes riesgos de gestión en “Riesgos Estratégicos y del Negocio”, en “Riesgos Financieros” y en “Riesgos generales o de Apoyo”.

Los Riesgos estratégicos y del negocio los podemos clasificar en:

- Riesgo Político y de país o macroeconómico o soberano (inflación o devaluación interna o de países vecinos, guerrilla, narcotráfico, terrorismo, recesión, impuesto, etc.)
- Riesgo de crédito (tasas de interés altas, desconfianza en el mercado, regulaciones estrictas, falsificación de documentos y corrupción en general).

- Riesgo de imagen (fusiones, reestructuraciones, manejo de cambio).
- Riesgo competitivo (calidad, precio, distribución, servicio, productos sustitutos, competidores potenciales).
- Riesgo regulatorio (impuestos, aranceles de aduana, restricciones, control de precios).
- Riesgo de Operación (proveedores, calidad, liquidez, producción, maquinaria, especialización de la mano de obra, convertibilidad, fraudes, etc.)
- Riesgo de Liquidez (financiaciones, exceso de activos improductivos, stock exagerados, poco apoyo financiero de sus dueños, inversiones inoficiosas con disponibilidad a largo plazo, etc.)
- Riesgo de desastres naturales (incendios, terremotos, huracanes, inundaciones, etc.)
- Riesgo fiduciario (inversiones a la baja, patrimonios autónomos inadecuados, comisiones onerosas, poca gestión fiduciaria, etc.)
- Riesgo Interbancario (intervención del gobierno, desencajes, colocaciones a largo plazo y captaciones a corto plazo, gestión inescrupulosa, etc.)
- Riesgo de intervención estatal (por desencajes, colocaciones sin análisis suficientes, corrupción, etc.)

Los riesgos financieros se clasifican en:

- Riesgos de interés (volatilidad de las tasas de interés)
- Riesgo cambiario y de convertibilidad (devaluación o revaluación de la moneda nacional con el dólar, otras monedas y ahora con el euro).

Los riesgos generales o de apoyo, en:

- Riesgo de Organización (estructura poco clara, ausencia de planificación, carencia o fallas en el sistema, mal clima laboral, malos canales de comunicación).
- Riesgo de Auditoría (Inherente, control y detección).
- Riesgo de Información (tecnológico, integridad información, comunicación y disponibilidad de información).
- Riesgo de Operaciones ilícitas (lavado de activos, fraudes y delitos financieros).

- Seguridades físicas y humanas. (contratación de personas sin investigación suficiente, problemas graves personales, plan de contingencia inadecuado, etc.

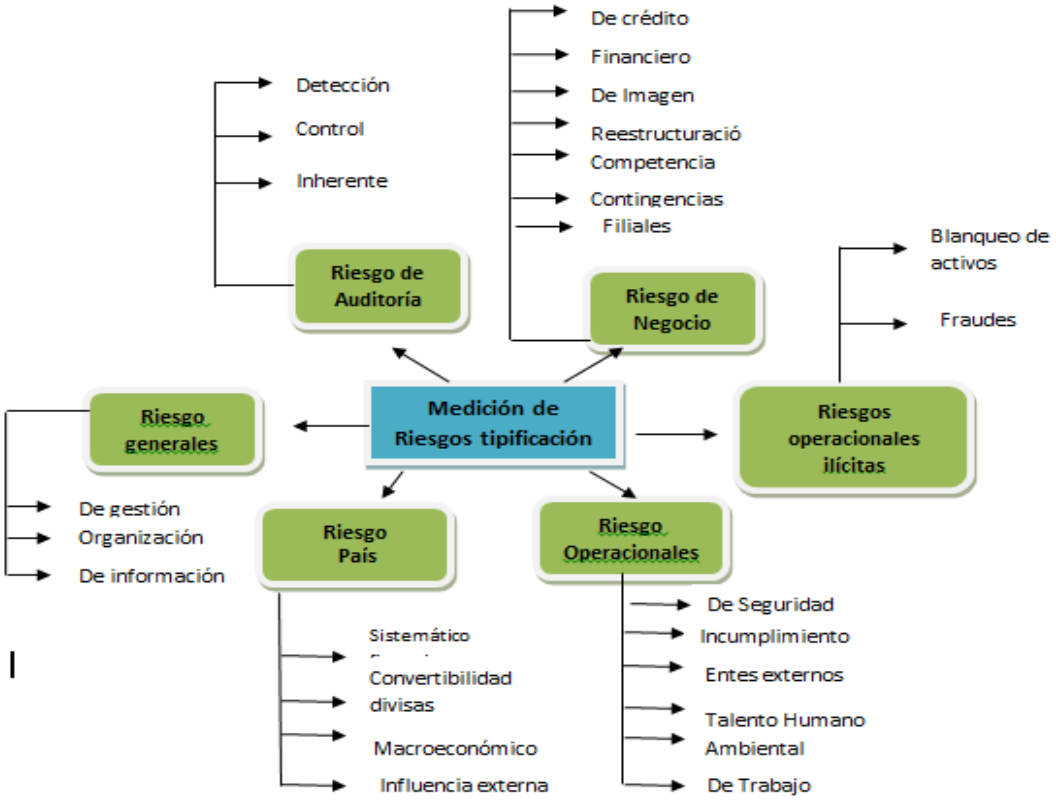


Figura 5, Medición de Riesgos-tipificación
Fuente: (Estupiñán Gaitán, 2006)

El Riesgo en el Sector Financiero

El riesgo en el sector financiero es el potencial de posibles pérdidas para cada entidad, para ellos es necesario en el corto plazo mantener la estabilidad financiera, protegiendo sus activos e ingresos de los riesgos que se está expuesta, y en el largo plazo minimizar las pérdidas ocasionadas por la ocurrencia de riesgo identificados en ilícitos o problemas que las hayan afectado sustancialmente.

Los riesgos en el sector financiero se dividen en “riesgos del negocio” y en “riesgos financieros”.

Los riesgos del negocio son los que se generan por producto de la actividad que realizan esas entidades, tales como el riesgo de mercado, el riesgo operativo, las operaciones bancarias, los fraudes, la falta de control de procedimientos, los problemas ocasionados por causas externas (terremoto, incendio entre otros) y los riesgos legales.

Los riesgos financieros son aquellos que se pactan, por ejemplo sí se tiene una hipoteca, se comparte el riesgo con el dueño de la casa, él fija una cuota inicial mientras se le presta el dinero, estos son riesgos que se miden sí se quiere asumirlos o no, y qué se quiere hacer con ellos. Entre estos están el riesgo crediticio, el cual es el más difícil de medir, el riesgo de liquidez o de Tesorería y el riesgo de mercado.

El problema como contingencia del Riesgo

La gama de riesgos que se enfrentan en una entidad depende, entre otros, de los siguientes factores:

- El volumen de los recursos.
- La complejidad de las actividades.
- Estructura organizativa.
- Magnitud de recursos y productos.
- Giro de la empresa.
- Nivel de tecnificación alcanzado.
- Lapso y momento evolutivo de la entidad.
- Marco competitivo nacional e internacional.
- La velocidad con que se desenvuelve la entidad

A la hora de analizar a fondo el término problema es necesario que antes estipulemos el origen etimológico del mismo. En este sentido, podemos decir que aquel se encuentra en el latín y más concretamente en la palabra problema. No obstante, también hay que determinar que la misma a su vez procede de un término griego

Un problema es un determinado asunto o una cuestión que requiere de una solución.

A nivel social, se trata de alguna situación en concreto que, en el momento en que se logra solucionar, aporta beneficios a la sociedad (como lograr disminuir la tasa de pobreza de un país o reconstruir edificios arrasados por un terremoto).

Tabla 1:

Diferencias entre problemas y Riesgos

DIFERENCIAS ENTRE PROBLEMAS Y RIESGOS		
Características	**Problema**	**Riesgos**
Controles insuficientemente aplicados	Detectivos y correctivos	Preventivos
Latencia en el tiempo	Temporal	Permanente
Posibilidad de medición	Más cuantificable	Menos cuantificable
Existencia	Real	Posible
Elemento generador	Agentes internos y externos	Por naturaleza
Asignación de prioridad a su estudio y tratamiento	De acuerdo a emergencia	Según experiencia e institución
Posibilidad de análisis para identificación de causas y repercusiones	Mayor	Menor
Evidencia	Existente	Inexistente
Momento de aparición	Presente	Futuro

Fuente: (Badillo, 2010)

Tabla 2:

Riesgos Agrupados por Nivel Jerárquico

RIESGOS AGRUPADOS POR NIVEL JERARQUICO		
HECHOS / CAUSAS	**JERARQUÍA**	**RIESGOS / EFECTOS**
	DIRECTIVO	
Indecisión		Estancamiento de la entidad
Desconocimiento del entorno		Sanciones Legales
Desconocimiento de la entidad		Inaplicabilidad de directrices
Imprecisión organizativa		Conflicto interfuncional
	GERENCIAL	
Descoordinación		Ineficiencia
Desvaloración		Desmotivación
Irresponsabilidad		Fuga de Recursos
Desinformación económica		Incosteabilidad
	ESPECIALISTA	
Desactualización		Inaplicabilidad
Desestandarización		Discontinuidad
Descalificación		Inoperabilidad
Desorientación		Incompatibilidad
Incompetencia		Incosteabilidad
	OPERATIVO	
Desacato		Conflicto Operativo
Desconocimiento		Errores
Deshonestidad		Fraude
Desinterés		Merma
Desobligación		Accidentes

Fuente: (Badillo, 2010)

Los elementos del riesgo son:

1. Indeterminación.- Existen por lo menos dos sucesos.
2. Pérdida.- Uno de los sucesos es indeseable.

Los tipos de riesgo son:

1. **Riesgo Inherente**.-Riesgo para la entidad en ausencia de cualquier acción realizada por la administración para alterar la probabilidad o el impacto.
2. **Riesgo Residual**.-Riesgo remanente después de la acción realizada por la administración para alterar su probabilidad o impacto.

1.3.3. Definición de control:

Es cualquier cosa que se haga para manejar riesgos de fracaso en la obtención de los objetivos corporativos.
Consiste en verificar si todo ocurre de conformidad con el plan adoptado, con las instrucciones emitidas y con los principios establecidos. Tiene como fin señalar las debilidades y errores para poder rectificarlos e impedir que se produzcan nuevamente… Henry Fayol

Elementos del concepto

Relación con lo planeado. El control siempre existe para verificar el logro de los objetivos que se establecen en la plantación.

Medición. Para controlar es imprescindible medir y cuantificar los resultados.

Detectar desviaciones. Una de las funciones inherentes al control es descubrir las diferencias que se presentan entre la ejecución y la planeación.

Establecer medidas correctivas. El objeto del control es prever y corregir los errores.

1.3.3.1. Importancia del Control

- Establece medidas para corregir las actividades, para que se alcancen los planes exitosamente.
- Se aplica a todo: a las cosas, a las personas y a los actos.

- Determina y analiza rápidamente las causas que pueden originar desviaciones, para que no se vuelvan a presentar en el futuro.

1.3.3.2. Principios del Control

1. **Equilibrio**. A cada grupo o delegación conferida debe proporcionársele el grado de control correspondiente.
2. **De los objetivos**. Se refiere a que el control existe en función de los objetivos, el control es un medio para alcanzar los objetivos preestablecidos.
3. **De la oportunidad**. El control para que sea eficaz, necesita ser oportuno, debe aplicarse antes de que se efectúe el error, de tal manera que sea posible tomar medidas correctivas con anticipación.
4. **De las desviaciones**. Todas las variaciones o desviaciones que se presenten en relación con los planes deben ser analizadas detalladamente, de tal manera que sea posible conocer las causas que las originaron, para poder tomar las medidas necesarias para evitarlas en el futuro.
5. **Costeabilidad.** El establecimiento de un sistema de control debe justificar el costo que este represente en tiempo y dinero, en relación con las ventajas reales que este reporte.
6. **De excepción.** El control debe aplicarse, preferentemente, a las actividades excepcionales o representativas, a fin de reducir costos y tiempo.
7. **De la función controlada**. La función controladora por ningún motivo debe comprender a la función controlada, ya que pierde efectividad el control. Una persona o la función que realiza el control no debe estar involucrada con la actividad a controlar.

1.3.3.3. Características del Control

El control es un factor imprescindible para el logro de los objetivos y por ello debe reunir ciertas características para ser efectivo.

- **Reflejar la naturaleza de la estructura organizacional**. Un sistema de control deberá ajustarse a las necesidades de la empresa y tipo de actividad que se desee controlar. Los

buenos controles deben relacionarse con la estructura organizativa y reflejar su eficacia, la función de control no puede suplir una organización precaria.

- **Oportunidad.** Un buen sistema de control debe manifestar inmediatamente las desviaciones, lo ideal es que las descubra antes de que se produzcan pues el control será útil en tanto proporcione información en el momento adecuado.

- **Accesibilidad**. Todo control debe establecer medidas sencillas y fáciles de interpretar para facilitar su aplicación. Es fundamental que los datos o informes de los controles sean accesibles para las personas a las que van a ser dirigidos. Las técnicas muy complicadas crean confusiones.

- **Ubicación estratégica**. Es imposible e incosteable implantar controles para todas las actividades de la empresa, por lo que es necesario establecerlos en ciertas áreas de acuerdo con criterios de valor estratégico.

Riesgo y Control – Visión del Riesgo

Tabla 3:

Visión del Riesgo

PASADO	PRESENTE Y FUTURO
• **El monitoreo de riesgo es una función exclusiva de los auditores internos.**	• El monitoreo de riesgo es responsabilidad de todos.
• **El riesgo es un factor negativo a ser controlado.**	• El riesgo puede considerarse también como una oportunidad.
• **Los riesgos son administrados en forma aislada.**	• Los riesgos son administrados a través de un proceso integrado.
• **La medición de riesgos es subjetiva.**	• El riesgo es casi siempre cuantificado

PASADO	PRESENTE Y FUTURO
• **Las funciones de administración de riesgos no están estructuradas y son divergentes.**	• La administración de riesgos es implementada dentro de una estructura integrada.
• **La revisión de riesgos se realiza periódicamente por la auditoría interna.**	• La revisión de riesgos acontece a través de autoevaluación constante.
• **El monitoreo de riesgo es una función exclusiva de los auditores internos.**	• El monitoreo de riesgo es responsabilidad de todos.

Fuente: (Auditoría, 2009)

1.3.4. Gestión de Riesgo

Figura 6, Metodología de Gestión de Riesgo

Fuente: (Badillo, 2010)

1.3.5. Administración de Riesgos

1. Mapa de Procesos (vinculado con los objetivos corporativos)
2. Inventario de Riesgos (general y detallado por procesos).
3. Análisis sobre Impacto - Probabilidad (votación).

4. Mapa de Riesgos.
5. Matriz de Administración de Riesgos (controles a implementarse para: evitar, reducir, compartir o aceptar el riesgo).

1.3.5.1. Mapa de Procesos:

Un mapa de procesos es un diagrama de valor, un inventario gráfico de los procesos de una organización.

Proporciona una perspectiva global – local, obligando a "posicionar" cada proceso respecto a la cadena de valor. Al mismo tiempo, relaciona el propósito de la organización con los procesos que los gestionan, utilizándose también como herramienta de consenso y aprendizaje. Existen diversas formas de diagramar un mapa de procesos. Uno de ellos y el más utilizado es el siguiente:

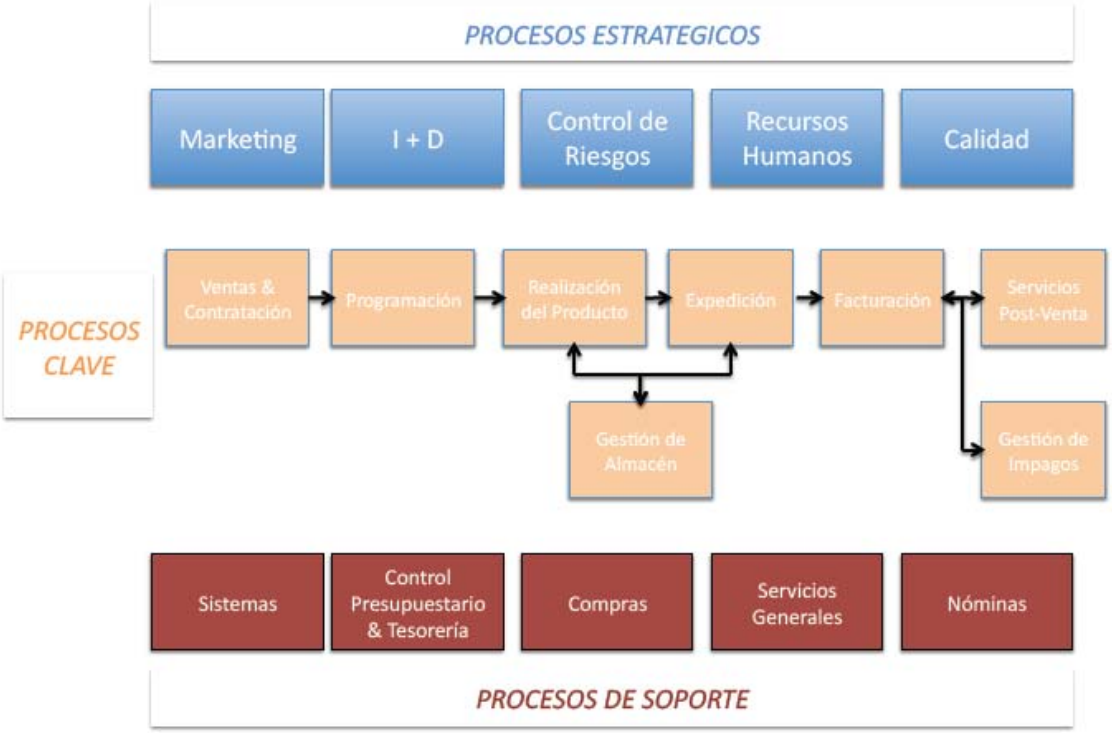


Figura 7, Mapa de procesos

Fuente: (Badillo, 2010)

Ejemplo de una empresa de Micro finanzas

Figura 8, Mapa de Procesos Ej. 1

Fuente: (Badillo, 2010)

1.3.5.2. Inventario de riesgos – Ejemplo de una empresa de Micro finanzas.

Un inventario de riesgos es la determinación y selección de los procesos que existen en la empresa validando a que grandes áreas pertenecen como son: procesos de controles internos, personas, tecnología e información y eventos externos.

INVENTARIOS DE RIESGOS OPERACIONALES	PROCESOS Y CONTROLES INTERNOS	PERSONAS	TECNOLOGIA DE INFORMACION	EVENTOS EXTERNOS
I. RIESGOS DEL ENTORNO				
Competencia				RO1
Innovación Tecnológica				RO2
Soberano/político				RO3
Legal				RO4
Regulatorio				RO5
Sector				RO6
Mercados financieros y de productos				RO7
Catástrofes				RO8
Pánico financiero				RO9
II. RIESGOS INTERNOS				
Procesos y Dirección				
Recursos humanos		RO10		
Diseño de procesos	RO11			
Tiempo de atención al cliente	RO12			
Cumplimiento y error humano		RO13		
Interrupción por falta de insumos	RO14			
Falla de productos o servicios	RO15			
Salud y seguridad	RO16			
Límite de autoridad		RO17		
Tercerización y subcontratación	RO18			
Tecnología de Información				
Integridad			RO19	
Confidencialidad y acceso			RO20	
Disponibilidad			RO21	
Honestidad y Conducta Etica				
Distorción de información externa e interna		RO22		
Fraude de empleados y terceros		RO23		
Actos ilegales		RO24		
Uso no autorizado		RO25		

Figura 9, Inventario de riesgos Ej. 1

Fuente: (Badillo, 2010)

Modelo de Riesgos ejemplo:

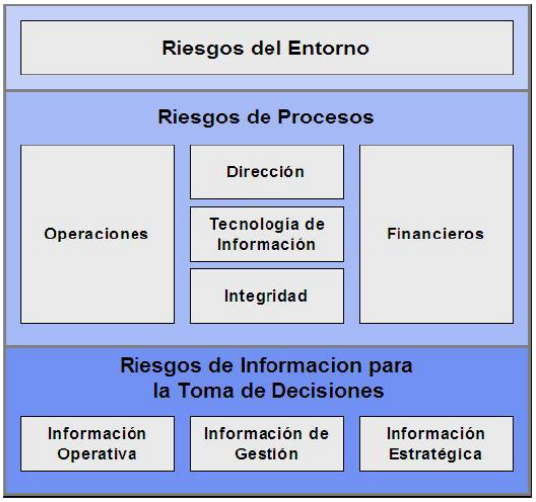


Figura 10, Modelo de Riesgos - Emp. Protiviti

Fuente: (Badillo, 2010)

Categorías de Riesgo

RIESGO ESTRATÉGICO

- Riesgo de reputación
- Imagen
- Pérdida de oportunidad

RIESGO FINANCIERO

- Riesgo de crédito
  - Riesgo de crédito directo
  - Riesgo de colocación
- Riesgo de Liquidez
  - Liquidez de mercado
  - Liquidez individual
- Riesgo de mercado
  - Riesgo de tasa
  - Riesgo de precio
- Riesgo de tipo de cambio

RIESGO DE OPERACIÓN

- Fallas en los sistemas
- Errores Humanos
- Procedimientos inadecuados
- Controles inadecuados
- Fraude
- Riesgo de desastres
- Riesgo Legal
- Riesgos regulatorios
  - Cambios regulatorios
  - Lavado de dinero

Figura 11, Categorías del Riesgo

Fuente: (Badillo, 2010)

1.3.5.3. Análisis sobre Impacto - Probabilidad

Una matriz de riesgo de probabilidad de impacto es una representación gráfica de dos dimensiones de los riesgos que enfrenta una organización o entidad, desde un individuo a

un planeta entero. La probabilidad de un evento se representa frente a los posibles efectos negativos de ese evento.

IMPACTO

Insignificante	Menor	Moderado	Mayor	Catastrófico
1	2	3	4	5

PROBABILIDAD

Raro	Improbable	Posible	Probable	Casi Seguro
1	2	3	4	5

1.3.5.4. Mapa de riesgos

Un mapa de riesgos es una herramienta que permite organizar la información sobre los riesgos de las empresas y visualizar su magnitud, con el fin de establecer las estrategias adecuadas para su manejo. Pueden representarse con gráficos o datos. Los gráficos corresponden a la calificación de los riesgos con sus respectivas variables y a su evaluación de acuerdo con el método utilizado en cada empresa.

Los datos pueden agruparse en tablas, con información referente a los riesgos; a su calificación, evaluación, controles y los demás datos que se requieran para contextualizar la situación de la empresa y sus procesos, con respecto a los riesgos que la puedan afectar y a las medidas de tratamiento implementadas.

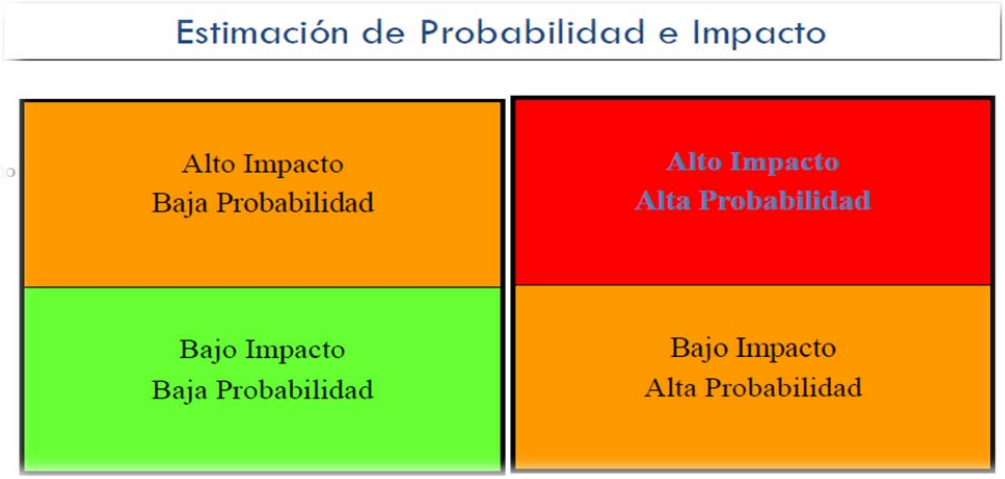


Figura 12, Mapa de Riesgos
Fuente: (Badillo, 2010)

1.3.5.5. Matriz de riesgos

Una matriz de riesgo constituye una herramienta de control y de gestión normalmente utilizada para identificar las actividades (procesos y productos) de una empresa, el tipo y nivel de riesgos inherentes a estas actividades y los factores exógenos y endógenos relacionados con estos riesgos (factores de riesgo). Igualmente, una matriz de riesgo permite evaluar la efectividad de una adecuada gestión y administración de los riesgos que pudieran impactar los resultados y por ende al logro de los objetivos de una organización.

La matriz debe ser una herramienta flexible que documente los procesos y evalúe de manera integral el riesgo de una institución, a partir de los cuales se realiza un diagnóstico objetivo de la situación global de riesgo de una entidad. La matriz de riesgos constituye una herramienta clave en el proceso de supervisión basada en riesgos, debido a que la misma nos permite efectuar una evaluación cualitativa o cuantitativa de los riesgos inherentes de cada actividad en estudio y la determinación del perfil de riesgo del proceso.
Los beneficios de la matriz entre otros, son los siguientes:

- Permite la intervención inmediata y la acción oportuna.
- Evaluación metódica de los riesgos.

- Promueve una sólida gestión de riesgos en las industrias.
- Monitoreo continuo.

De esta manera la matriz de riesgo permite establecer de un modo uniforme y consistente el perfil de riesgo de cada uno de los procesos y permite profundizar en el propósito de establecimiento de planes de supervisión a fin de que se ajusten a las características específicas de cada empresa.

MATRIZ DE RIESGOS

PROCESO: CRÉDITOS SUB PROCESO: FORMALIZACION DE GARANTIAS

1. EVENTOS DE RIESGO	2. INCLUIR EN EL ANALISIS?	EVALUACION 3. PROBABILIDAD	4. IMPACTO	5. NIVEL DE RIESGO	1. CONTROLES ESPECIFICOS	2. TIPO DE CONTROL	3. MANUAL (M) / SISTEMA (S)	4. SITUACION DE LA IMPLEMENTACION	5. EFECTIVIDAD DEL DISEÑO	Realizado Por	OBSERVACION
Riesgo No.13 : Incumplimiento y error humano											
a) Error en el registro en el sistema de los datos de las garantías.	S	4	3	A	a.1) Cotejar periódicamente los reportes del sistema contra los documentos físicos y emitir un reporte con los resultados.	RC	M	IMP	DEF	Administrador de Créditos	
					a.2) Revisar aleatoriamente los expedientes de créditos con garantía y hacer seguimiento a los resultados obtenidos.	RC	M	IMP	DPE	Auditoría Interna	
b) No bloquear, o desbloquear incorrectamente una cuenta de depósito a plazo fijo otorgada en garantía.	S	4	2	A	b.1) Asignar controles de bloqueo en el sistema según perfiles.	RP	S	IMP	DEF	Administrador de Créditos \ Jefe de Operaciones	
Riesgo No.23 : Fraude de empleados y terceros											
a) Presentación de información alterada o documentos falsos.	S	4	2	A	a.1) Consultar a RENIEC, SUNAT, SUNARP vía Internet.	RP	M	IMP	DEF	Administración de Créditos \ Asesoría Legal	
					a.2) Consultar a centrales de riesgo (v.g Infocorp).	RP	M	IPP C3B	DPE	Jefe de Créditos\Analistas	C3B: Solamente acceso a SBS. Infocorp o Certicom en evaluación
					a.3) Revisar y aprobar los créditos con garantías.	RP	M	IMP	DEF	Jefe de Negocios	
					a.4) Revisar aleatoriamente los de expedientes de créditos con garantía y hacer seguimiento a los resultados obtenidos.	RC	M	IMP	DPE	Auditoría Interna	

Figura 13, Matriz de Riesgos

Fuente: (Badillo, 2010)

1.4. Gestión de Riesgos en las Industria: Banca y Finanzas.

Basilea II

El acuerdo de Basilea II destaca la importancia de la gestión de riesgos en las entidades financieras a través de los tres pilares que describe:

Pilar I: el cálculo de los requisitos mínimos de capital; considerando:

- Riesgo de crédito.
- Riesgo de mercado.
- Riesgo de tipo de cambio.
- Riesgo operacional.

Pilar II: el proceso de supervisión de la gestión de los fondos propios
Pilar III: La disciplina de mercado

1.4.1. Gestión de Riesgo Operacional en el Ecuador

La resolución JB-2005-834 establece lineamientos para la gestión del riesgo operacional considerando sus 4 factores:

1. Personas:

Las instituciones controladas deben administrar el capital humano de forma adecuada, e identificar apropiadamente las fallas o insuficiencias asociadas al factor "personas", tales como: falta de personal adecuado, negligencia, error humano, nepotismo de conformidad con las disposiciones legales vigentes, inapropiadas relaciones interpersonales y ambiente laboral desfavorable, falta de especificaciones claras en los términos de contratación del personal, entre otros.

Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las instituciones controladas deberán definir formalmente políticas, procesos y procedimientos que aseguren una apropiada planificación y administración del capital humano, los cuales considerarán los procesos de incorporación, permanencia y desvinculación del personal al servicio de la institución.
Dichos procesos corresponden a:

Los procesos de incorporación.- Que comprenden la planificación de necesidades, el reclutamiento, la selección, la contratación e inducción de nuevo personal;

Los procesos de permanencia.- Que cubren la creación de condiciones laborales idóneas; la promoción de actividades de capacitación y formación que permitan al personal aumentar y perfeccionar sus conocimientos, competencias y destrezas; la existencia de un sistema de valuación del desempeño; desarrollo de carrera; rendición de cuentas; e incentivos que motiven la adhesión a los valores y controles institucionales; y,

Los procesos de desvinculación.- "Que comprenden la planificación de la salida del personal por causas regulares, preparación de aspectos jurídicos para llegar al finiquito y la finalización de la relación laboral". (Superintendencia de Bancos y Seguros de la República del Ecuador, 2005)

2. Procesos:

Con el objeto de garantizar la optimización de los recursos y la estandarización de las actividades, las instituciones controladas deben contar con procesos definidos de conformidad con la estrategia y las políticas adoptadas, que deberán ser agrupados de la siguiente manera:

Procesos gobernantes o estratégicos.- Se considerarán a aquellos que proporcionan directrices a los demás procesos y son realizados por el directorio u organismo que haga sus veces y por la alta gerencia para poder cumplir con los objetivos y políticas institucionales. Se refieren a la planificación estratégica, los lineamientos de acción básicos, la estructura organizacional, la administración integral de riesgos, entre otros;

Procesos productivos, fundamentales u operativos.- Son los procesos esenciales de la entidad destinados a llevar a cabo las actividades que permitan ejecutar efectivamente las políticas y estrategias relacionadas con la calidad de los productos o servicios que ofrecen a sus clientes; y,

Procesos habilitantes, de soporte o apoyo.- "Son aquellos que apoyan a los procesos gobernantes y productivos, se encargan de proporcionar personal competente, reducir los

riesgos del trabajo, preservar la calidad de los materiales, equipos y herramientas, mantener las condiciones de operatividad y funcionamiento, coordinar y controlar la eficacia del desempeño administrativo y la optimización de los recursos".
(Superintendencia de Bancos y Seguros de la República del Ecuador, 2005)

3. Tecnología de la Información

Las instituciones controladas deben contar con la tecnología de información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable; evitar interrupciones del negocio y lograr que la información, inclusive aquella bajo la modalidad de servicios provistos por terceros, sea íntegra, confidencial y esté disponible para una apropiada toma de decisiones.

Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las instituciones controladas deberán definir formalmente políticas, procesos y procedimientos que aseguren una adecuada planificación y administración de la tecnología de información. (Superintendencia de Bancos y Seguros de la República del Ecuador, 2005)

4. Eventos Externos

En la administración del riesgo operativo, las instituciones controladas deben considerar la posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos a su control, tales como: fallas en los servicios públicos, ocurrencia de desastres naturales, atentados y otros actos delictivos, los cuales pudieran alterar el desarrollo normal de sus actividades. Para el efecto, deben contar con planes de contingencia y de continuidad del negocio. (Superintendencia de Bancos y Seguros de la República del Ecuador, 2005)

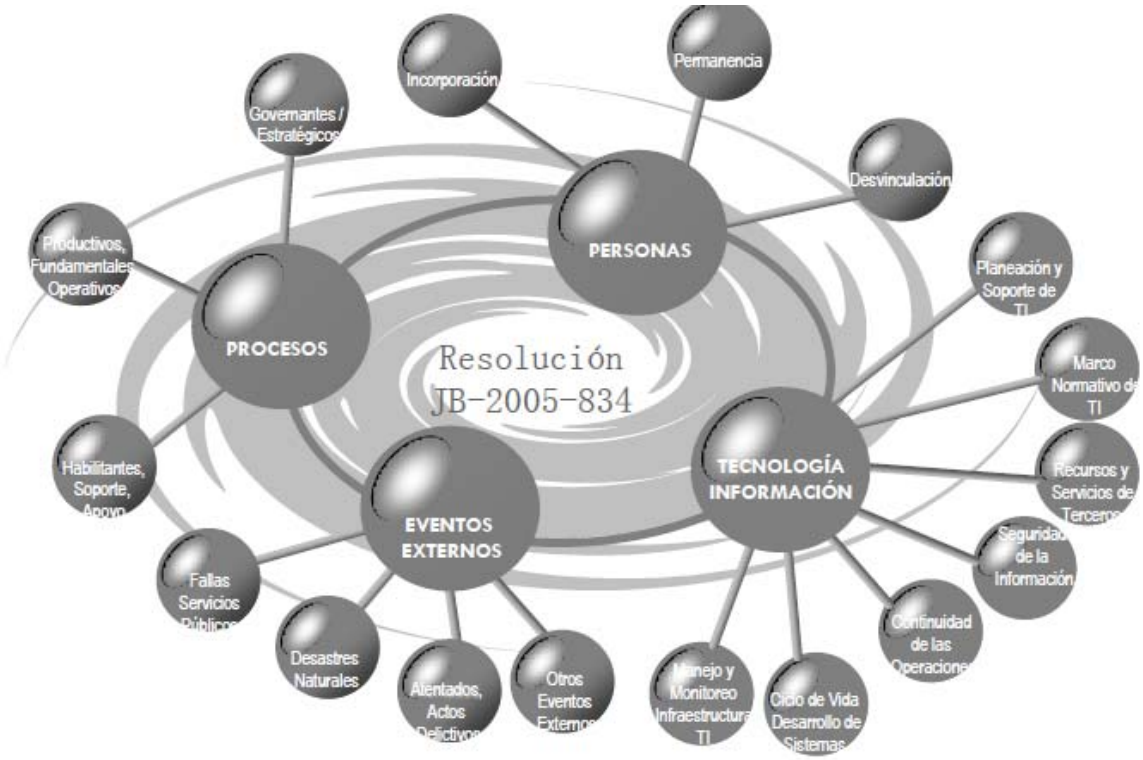


Figura 14, Gestión de Riesgos según la S.B.S.

Fuente: (Badillo, 2010)

Reporte de los riesgos empresariales 2010 (Ernest & Young)

Dentro de los riesgos empresariales tenemos un top de los riesgos de acuerdo a un ranking de evaluación como se describe a continuación:

Top 10 Risk (rankings in parentheses)

- Regulación y cumplimiento (2)
- Acceso al crédito (1)
- Lenta recuperación o doble recesión (sin cambio)
- Gestión de Talento (7)
- Mercados emergentes (12)
- Reducción de costos (sin cambio)
- Participantes no tradicionales (5)
- Ambientalismo radical (4)
- Riesgo de aceptación social y responsabilidad social empresarial (nuevo)

- Ejecución de alianzas y transacciones (8)

Figura 15, Top 10 Risk

Fuente: (Ernst&Young, 2010)

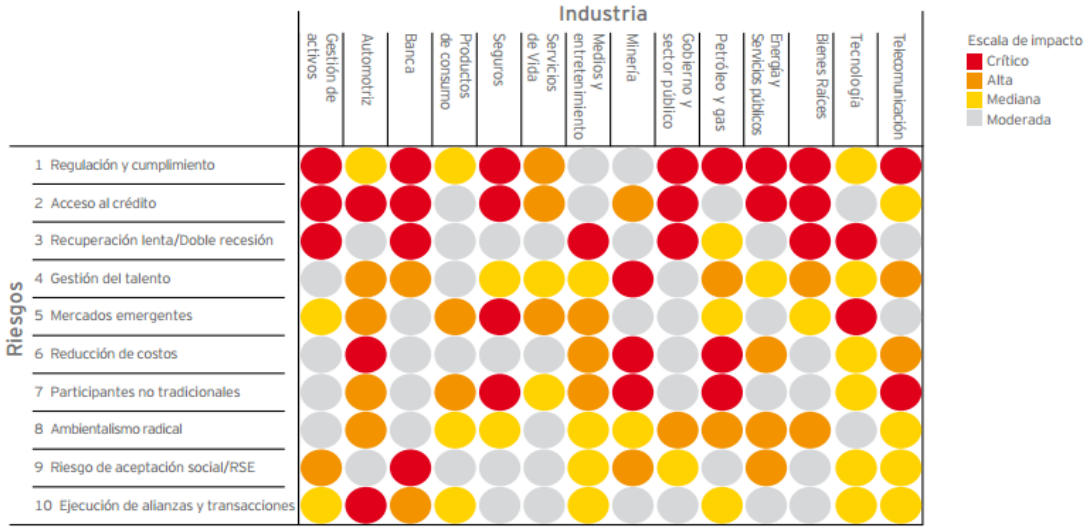


Figura 16, Matriz de Riesgos

Fuente: (Ernst&Young, 2010)

Bussines Risk report 2010 (Ernst & Young)

Top 10 Risk – Banking

1. Riesgos de cumplimiento y reglamentación
2. Crisis macroeconómicas o geopolíticas
3. Riesgo reputacional.
4. Problemas en la calidad y el valor residual del crédito
5. Recuperación débil recesión secundaria.
6. Riesgo de capital humano, incluyendo estructuras de compensación desalineadas.
7. Gestión corporativa y fallas de control interno.
8. Cambio organizacional.
9. Riesgos en Tecnologías de Información.
10. Reducción de las ganancias y valoraciones.

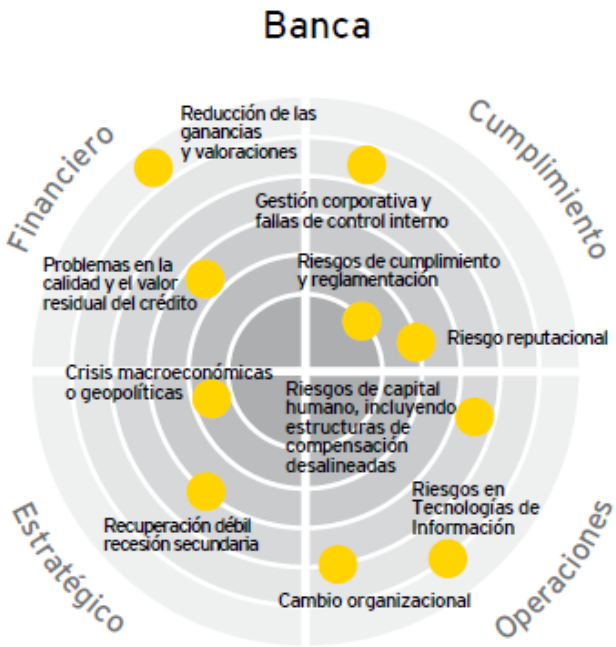


Figura 17, Top 10 de los Riesgos Bancarios

Fuente: (Ernst&Young, 2010)

1.4.2. Bancos centran esfuerzos en la gestión de riesgos

La crisis cambió dramáticamente la actitud y el enfoque de los bancos hacia el riesgo. Muchas de las entidades bancarias han adoptado o están adoptando un enfoque más integral, que requiere la implantación de una cultura que genere conciencia sobre la responsabilidad en la identificación del riesgo, de todos los niveles, independientemente de su jerarquía.

Para conocer las principales acciones que los bancos están llevando a cabo, en materia de administración del riesgo, en Ernst & Young entrevistó a 48 ejecutivos senior de 36 de las principales instituciones bancarias del mundo. En conjunto, señalaron cuatro áreas vitales, interrelacionadas, para alcanzar pro-actividad y efectividad en la administración del riesgo.

Las iniciativas abarcan desde el refuerzo inmediato de los controles hasta cambios culturales que exigirán un plazo mayor. En ambos extremos, una mayor y mejor coordinación y alineamiento entre las áreas de riesgo y finanzas serán determinantes. Los banqueros entrevistados priorizaron el reforzamiento de controles (50%) y el cambio cultural (40%). En tercer lugar ubicaron la reevaluación de roles y responsabilidades (23%) y en cuarto lugar una comunicación más rápida y efectiva (15%). (Ernst&Young, 2010)

Los reportes se han vuelto cualitativamente más ricos e importantes. Los informes que proporcionan valor real y acciones a tomar son los más solicitados, un cambio evidente del antiguo modelo "vertedero de datos" que caracterizaba a los reportes de riesgos en el pasado. Los bancos buscan más claridad, transparencia y un entendimiento interpretativo en los reportes a las juntas directivas y líderes senior.

Entre los pasos que los ejecutivos recomiendan para afianzar la dupla finanzas-riesgos están:

- Realizar proyecciones de liquidez.
- Compartir información sobre riesgos.

- Involucrar las áreas de riesgos y finanzas en la evaluación de potenciales adquisiciones.
- Crear procesos y equipos conjuntos para apoyar la publicación de información financiera.
- Reportar el impacto sobre ganancias o pérdidas como parte de la definición y el análisis de riesgo.
- Apalancar las competencias de cada área.

- Posiblemente el mayor desafío para conseguir esta mejor integración entre riesgos y finanzas sea eliminar, o al menos reducir, las diferencias culturales. Mientras en la mayoría de los bancos la tendencia del área de finanzas es mirar lo que ha ocurrido en el pasado, tal y como se refleja en los números, la administración de riesgos tiende a ver hacia el futuro.

- De ahí que para trabajar en conjunto, efectivamente, los equipos de riesgo y de finanzas necesitan un lenguaje común, una serie de definiciones que ambos comprendan y un entendimiento claro sobre las diferentes responsabilidades de cada uno.

- Se requerirá, además, de un sistema a nivel de empresa que proporcione números que sirvan para todos. Para muchos ejecutivos, es clave la sincronización de los sistemas de riesgos y finanzas y determinar cuál información debe ser compartida y de qué manera.

- Le corresponde a la alta administración establecer los lineamientos y comunicar lo que se espera de la colaboración efectiva entre finanzas y riesgos la forma en que esta cooperación debe permear a toda la organización. Implantar una cultura donde el riesgo sea un asunto de todos, requiere de acciones claras, transparentes y contundentes que sean reforzadas con mensajes clave por parte de la alta dirección. Es acá de dónde deben salir las señales del cambio.

1.5. Cultura Organizacional

En la medida que avanza el siglo XXI, varias tendencias económicas y demográficas están causando un gran impacto en la cultura organizacional. Estas nuevas tendencias y los cambios dinámicos hacen que las organizaciones y las instituciones tanto públicas, como privadas se debatan en la urgente necesidad de orientarse hacia los avances tecnológicos.

Desde la perspectiva más general, la globalización, la apertura económica, la competitividad son fenómenos nuevos a los que se tienen que enfrentar las organizaciones. En la medida que la competitividad sea un elemento fundamental en el éxito de toda organización, los gerentes o líderes harán más esfuerzos para alcanzar altos niveles de productividad y eficiencia.

Las organizaciones son la expresión de una realidad cultural, que están llamadas a vivir en un mundo de permanente cambio, tanto en lo social como en lo económico y tecnológico, o, por el contrario, como cualquier organismo, encerrarse en el marco de sus límites formales. En ambos casos, esa realidad cultural refleja un marco de valores, creencias, ideas, sentimientos y voluntades de una comunidad institucional.

Hoy en día es necesario que las organizaciones diseñen estructuras más flexibles al cambio y que este cambio se produzca como consecuencia del aprendizaje de sus miembros. Esto implica generar condiciones para promover equipos de alto desempeño, entendiendo que el aprendizaje en equipo implica generar valor al trabajo y más adaptabilidad al cambio con una amplia visión hacia la innovación.

La cultura determina la forma como funciona una empresa, ésta se refleja en las estrategias, estructuras y sistemas. Es la fuente invisible donde la visión adquiere su guía de acción. El éxito de los proyectos de transformación depende del talento y de la aptitud de la gerencia para cambiar la cultura de la organización de acuerdo a las exigencias del entorno. Al respecto Deal y Kennedy (1985) observan a la cultura organizacional como "la conducta convencional de una sociedad que comparte una serie de valores y creencias particulares y

éstos a su vez influyen en todas sus acciones". Por lo tanto, la cultura por ser aprendida, evoluciona con nuevas experiencias, y puede ser cambiada si llega a entenderse la dinámica del proceso de aprendizaje.

Dentro del marco conceptual, la cultura organizacional tiene la particularidad de manifestarse a través de conductas significativas de los miembros de una organización, las cuales facilitan el comportamiento en la misma y, se identifican básicamente a través de un conjunto de prácticas gerenciales y supervisoras, como elementos de la dinámica organizacional. Al respecto Guerin (1992) sostiene que es importante conocer el tipo de cultura de una organización, porque los valores y las normas van a influir en los comportamientos de los individuos. (Monografias.com)

La definición que le podemos aplicar a la cultura organizacional es la unión de normas, hábitos y valores que de una forma u otra, son compartidos por las personas y/o grupos que dan forma a una institución, y que a su vez son capaces de controlar la forma en la que interactúan con el propio entorno y entre ellos mismos. Es decir, el comportamiento de la empresa dependerá de la forma en la que se apliquen unas normas u otras por parte de sus integrantes. (Díaz, 2013)

Es importante la Cultura Organizacional dentro de una empresa ya que es tremendamente útil para poder detectar problemas y encontrar una solución lo antes posible. Con ella se pueden formar grupos de trabajo con aptitudes similares con el fin de ofrecer un rendimiento mucho más productivo.

Dentro del concepto de cultura organizacional hay que considerar tanto aquellos aspectos intangibles, tales como el conocimiento o los mismos valores, como aquellos aspectos tangibles propios del sistema.

La cultura organizacional otorga a sus miembros la lógica de sentido para interpretar la vida de la organización, a la vez que constituye un elemento distintivo que le permite diferenciarse de las demás organizaciones.

Cultura organizativa constituye un sistema de significados que son compartidos de manera muy profunda, desde la alta dirección hasta la base operativa de una empresa, tratándose de algo implícito, intangible e informal que la diferencia de las demás y, que dada su preponderancia y espíritu integrador de un universo simbólico que es externo e interno, asemeja en concordancia a ella a actitudes y conductas de los miembros de las organizaciones, y puede fortalecer supuestamente a todo el conglomerado de reglas, normativas, procesos, sistemas y estructuras de poder que esquematizan, especifican y condicionan a la toma de decisiones gerenciales y demás políticas, prácticas, funcionamiento y actuaciones de la organización. (Geovanni Basabe, 2013)

La Cultura como proceso

La cultura es un proceso, entendido como fases sucesivas de un fenómeno compartido por todos los miembros de la organización, a partir del cual se genera sentido. Esto implica reconocerla como un emergente, lo cual no excluye su condición de relativamente estable, ya que la noción de proceso alude tanto a la idea de reconfiguración como a la de dicha estabilidad.

En todo sistema cultural coexisten culturas locales o sectoriales y para que dicha coexistencia sea posible no deben entrar en contradicción con la identidad propia de la organización.

Es posible reconocer distintas categorías de sistemas culturales, como son:

- Fuertes o débiles: según la intensidad con que los rasgos culturales impulsan las conductas de los individuos. Cuanto mayor sean esos rasgos, se impondrán más firmemente sobre las conductas, no sólo de los integrantes de la organización, sino sobre otros pertenecientes a otras organizaciones.

- Concentradas o fragmentadas: según el grado de autodeterminación de la cultura por parte de las unidades componentes de una organización.

- Tendientes al cierre o a la apertura: según la permeabilidad del sistema a los cambios del entorno.

- Autónomas o reflejas: en virtud de si las pautas son singulares o imitación de un modelo externo.

1.5.1. Tipos de cultura

La cultura del PODER:

- Juego de negociación y compromiso entre individuos, grupos y coaliciones en conflicto.
- Fuente central de poder.
- El crecimiento de la organización depende de la capacidad de la persona que está en el centro.
- Organización politizada.
- Cultura orgullosa y fuerte.
- Motivación por dinero o símbolos.

La cultura de la FUNCIÓN:

- Típica de las burocracias.
- Es lógica y racional.
- Coexisten funciones especializadas.
- Coordinadas por pequeños grupos en la cima de la organización.
- Poder = posición formal.
- Conocimiento de las normas y especialización.
- “Yo soy mi puesto”.

La cultura de la PERSONA:

- El individuo es el eje principal.
- Diseñada para servir a sus miembros.
- Aplicable a organizaciones de profesionales.

- Existe gran autonomía decisoria individual.
- Sus integrantes se destacan por sí mismos.
- Cuesta lograr la identificación con la organización.
- Influencia y negociación "uno a uno".

La cultura de la TAREA:

- La capacidad técnica es la fuente del poder.
- Se aplica en estructuras matriciales y virtuales.
- Se comparte el conocimiento.
- Apta para la resolución de problemas.
- Manejo de proyectos complejos e innovadores.
- No existen privilegios (edad, antigüedad, etc.)
- Cultura de equipo y muy adaptable. (Taller de Producción de mensajes)

1.5.2. Desarrollo de la cultura de una organización

Los puntos básicos para el desarrollo de la cultura de una empresa son:

- Orientar a la empresa hacia la acción, con el fin de que se cumpla.
- Orientar al cliente, todos los recursos y el personal de la compañía que dirijan sus actividades cotidianas a la satisfacción de las necesidades del cliente.
- Tener autonomía y decisión para fomentar el surgimiento de líderes e innovadores para la organización.
- Producir a través de la gente, se debe considerar a las personas como el activo más importante de la empresa; además, considerar como inversión el dinero destinado hacia ellos como fuente fundamental de mejoramiento.
- Comprometerse con los valores de la entidad, se debe hacer desde los niveles más superiores de la compañía.
- Estar pendientes de la organización, teniendo conocimiento de la misma, ya sea de sus fortalezas, debilidades, oportunidades o amenazas.

Para que la cultura de determinada organización se desarrolle, se debe promover el surgimiento de líderes que den aportes importantes a la empresa, pero sobre todo, se deben comprometer con los valores que posean a nivel organizacional, desde la máxima autoridad hasta todos sus subordinados, porque si las autoridades no lo hacen menos que los hagan los otros.

El desarrollo de la cultura organizacional permite a los integrantes de la entidad ciertas conductas inhibiendo otras. La cultura laboral alienta la participación y la conducta madura de los empleados y si estos se comprometen con la empresa y son responsables es porque la cultura de la organización se los permite; por lo que se debe considerar a la cultura como una fortaleza que encamina a las empresas hacia la excelencia y al éxito.

¿Cómo comienza la cultura de una empresa?

Robbins (1987: 446), plantea que la primera fuente para la formación de una cultura, son sus fundadores, porque ellos transmiten su sistema de creencias, actitudes y valores a sus primeros empleados, los que a su vez la adoptan y la van transmitiendo con el tiempo a los miembros que van formando parte de la empresa.

La herencia que dejan los fundadores son los factores determinantes en el momento de la concepción como es la estructura dominante que expresan los valores centrales que comparten la mayoría de los miembros de la organización como: la autonomía individual, la estructura o normas que establece la empresa, el apoyo, esto se refleja en la ayuda que brinda el gerente a su subordinado, la identidad que siente el empleado en el grupo y a nivel organizacional, el desempeño que realizan los trabajadores para realizar bien sus funciones, deben ser motivados con premios, incentivos, regalos, entre otros, la tolerancia al conflicto es parte de los empleados para evitar problemas a lo interno de la empresa, la tolerancia al riesgo es el miedo que tienen a la innovación de los retos que imponen riesgos de determinada actividad.

Cada organización crea una cultura que le es propia y se va desarrollando a medida que los nuevos miembros del grupo aprenden la conducta que es indispensable para que el grupo funcione, es por esta razón que obtienen el éxito deseado y contribuyen con las metas que se han propuesto.

Una empresa crea una cultura con el fin que los individuos se sientan identificados con ella, y que esta les otorga seguridad y respaldo.

Según (Kopelman, A., & R., 1990) la afluencia de planteamientos o criterios, también se ha visto obstaculizada al abordar la cultura desde los paradigmas "racionalista" y "constructivista" de la psicología organizacional.

a) De acuerdo con el paradigma racionalista, la cultura organizativa se identifica como una variable más de la empresa, capaz de ser gestionada para lograr determinados estándares de eficiencia económica, sobretodo, cuando se desea introducir en los fundamentos de la dirección la idea de implantar, de una forma adecuada, un modelo estratégico de gestión de la Calidad Total, que involucre no solo a los atributos de un producto, sino a la organización en su conjunto de manera especial a los recursos humanos de la empresa.

b) Mientras que para el paradigma constructivista no es que la empresa posea una cultura sino que la es en sí, sobre todo al tratarse de determinadas consistencias filosóficas que, al estar ligadas al logro de resultados, identifican plenamente a la empresa como tal.

2. ENFOQUE DE AUDITORÍA INTERNA Y LA GESTIÓN DE RIESGOS (COSO ERM)

2.1. Enfoque de la Auditoría y la Gestión de Riesgos (ERM)

A través del tiempo los problemas de control interno en las empresa se ha preocupado de la gerencia moderna, así como la responsabilidad de implementar nuevas formas de mejorar y perfeccionar dichos controles, es importante por cuanto el control interno es fundamental para que la empresa logre alcanzar a través de una evaluación de su misión y visión el logro de sus objetivos y metas trazadas, ya que sin ello es imposible definir las medidas para adoptar y así alcanzar y evaluar el grado de cumplimiento.

Rol del Auditor Interno

Cuando se habla del rol del Auditor Interno en los procesos de auto-evaluación de controles, se parte de la premisa que en las organizaciones ya existe determinada cultura administrativa, mediante la cual sus integrantes tienen claramente entendido lo que es el proceso de control, la importancia y beneficio de un buen sistema del control, así como de su propia responsabilidad sobre la eficiencia y eficacia del funcionamiento del proceso respectivo.

Esto implica que la administración ya debe mantener un Modelo de Control, adecuado las características de la organización, cuya implantación debe ser apoyada por una amplia difusión y un programa de capacitación para todos los involucrados en el proceso de control, a fin de propiciar un cambio en la manera de pensar o actuar del personal, haciendo que asuman el papel de propietarios del control interno y proporcionarles apoyo y orientación en el cumplimiento de sus metas y objetivos.
La actividad de la Auditoría Interna es lograr el suficiente grado de reconocimiento en la organización, que le permita impulsar y liderar los procesos de Autoevaluación de riesgos y

de Control, este reconocimiento se alcanza cuando la participación de Auditoría Interna aporta de manera tangible un valor agregado, mediante su apoyo a la mejora de las operaciones y de los resultados, así como el fortalecimiento de los procesos de administración de riesgos, control y gobierno corporativo.

Enfoques tradicionales:

La Auditoría Interna ha sido considerada universal como una evaluación establecida dentro de la empresa, para examinar, evaluar y monitorear adecuadamente y con eficacia el sistema de control interno y el contable, también se le han asignado funciones para determinar la eficacia y eficiencia económica de los sistemas operacionales y los controles gerenciales encaminados a los flujos financieros.

La auditoría interna nació por iniciativa de la auditoría externa de estados financieros contables, siendo la principal fuente de reclutamiento de auditores internos las grandes firmas de contadores públicos independientes y es así también que las normas del instituto de Auditores Internos I.A.I. guardan cierto paralelismo con las Normas de Auditoría generalmente aceptadas N.A.G.A. por lo que la única diferencia sustancial entre ambas actividades era el aspecto formal, la auditoría interna mantiene una relación de dependencia laboral con la empresa, mientras que la externa se identifica como independiente. (Estupiñán Gaitán, 2006)

A partir de la década de los noventa, por los cambios tecnológicos, las nuevas teorías de administración y control, como la globalización de la economía, el ambiente del manejo de los negocios sufrió cambios de importancia, que afectaron paralelamente a la auditoría interna a nivel mundial como fueron los conceptos de valor agregado, servicios al cliente, globalización de los mercados, estructuras orgánicas planas y matriarcales, trabajo en equipo, rápida reacción al cambio en los negocios, riesgos del negocio y desarrollos en tecnología de la información.

Nuevos enfoques de Auditoría Interna

Como resultado de la aplicación de los conceptos tradicionales, afectaron la aplicación de la auditoría interna, apareciendo nuevas prácticas acordes a los cambios, encaminadas a que se hicieran revisiones que generan alto valor agregado, las cuales se basan en los siguientes factores:

Servicio al cliente:

La empresa auditada es un cliente o usuario, no obstante tener dependencia laboral, lo que obliga a la auditoría tener permanentemente contacto con todas las dependencias de la organización para lograr mejoramiento de los procesos operativos y una comunicación continua con todos ellos dentro del proceso de la auditoría, para:

a) Transmitir claramente los objetivos de la auditoría.
b) Involucrar a las gerencias de área en la elaboración de los programas de trabajo;
c) Tener en cuenta la opinión de las gerencias y departamentos y otros niveles cuanto al ambiente de control, procesos críticos y riesgos relevantes en las áreas a su cargo.
d) Discutir con la gerencia los hallazgos y deficiencias en la medida en que se van detectando, trabajar conjuntamente con ellos para proponer las medidas correctivas; y,
e) Obtener una retroalimentación de los auditados en cuanto al impacto de la auditoría y la calidad de los servicios profesionales de la A.I.

Calidad total y mejoramiento continuo. Utilizar el benchmarking o comparación con las prácticas de las mejores empresas del mundo en cuanto a sus auditorías internas y aplicar indicadores de desempeño en el desarrollo de la auditoría interna.

Entrenamiento de futuros gerentes para el negocio. Con base en el conocimiento global de la empresa que debe tener los auditores internos y que se aplican en el desarrollo del

trabajo, debe utilizarse la auditoría interna como una plataforma de entrenamiento y capacitación para los futuros gerentes para la administración del negocio.

La evaluación de riesgos. Aplicar el enfoque de evaluación de riesgos de cumplimiento, de operación y de información, para:

a) Concentrar los recursos y revisiones de auditoría hacia las áreas de la organización que generen más valor, respondiendo a los mecanismos que posee la empresa para evaluar, detectar y establecer prioridades en materia de riesgos.
b) Reportar la magnitud y tipo de riesgos que la organización afronta, así como las acciones requeridas para la minimización de los mismos;
c) Transmitir la experiencia del auditor en la identificación de riesgos durante las auditorías;
d) Evolucionar del dominio de los controles al dominio de riesgos.
e) Promover el entendimiento organizacional sobre el enfoque y exposición de riesgo y su manejo; y
f) Contribuir al mejoramiento del manejo de riesgo y de los sistemas de control.

Mejoramiento constante. Para optimizar el servicio a sus clientes, es indispensable que el auditor interno debe:

a) Conocer el negocio y la organización;
b) Aplicar un enfoque proactivo, es decir que no se conforme únicamente con detectar problemas sino que, en lo posible, proponga las respectivas soluciones;
c) Ser creativo, objetivo y conciso;
d) Mantener continua comunicación con los auditados; y
e) Aplicar una visión global del negocio y del ambiente de control.

Tecnología de Información. Se debe incorporar a la auditoría interna, las últimas tecnologías de aplicación de equipos y software especiales que existen o se crean para sus labores de control y asesoría a la administración y así incrementar la productividad de las

dependencias de la empresa de la empresa, utilizando las nuevas tecnologías para llevar un seguimiento de las actividades del proceso de auditoría, para automatizar rutinas de trabajo, para acceder a bases de datos compartidas y para presentar y difundir los hallazgos de auditoría.

En el nuevo enfoque la auditoría moderna debe examinar:

- La eficacia de la gestión considerando los resultados alcanzados
- Su eficiencia, evaluando los recursos aplicados para ello, investiga las causas de los eventuales problemas
- Ineficacias o ineficiencias que pueda encontrar
- Y propone caminos para superarlos.
-

Se debe tener en cuenta la incidencia cada vez mayor de la informática en la gestión, profundizando en el análisis de los sistemas y de la actividad informática en general; y considerar los temas ambientales.

No le deben ser ajenos a los programas de aseguramiento de la calidad en los que su actividad suele tener un papel importante - ni los procesos de autoevaluación del control interno - Control self assessment - en los que por sus conocimientos y experiencia en el tema, puede oficiar el líder. (Estupiñán Gaitán, 2006)

La auditoría interna es una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización. Ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno corporativo. (Instituto de Auditores Internos, Rol del Auditor Interno en el ERM.pdf)

La auditoría interna revisa la confiabilidad e integridad de la información, el cumplimiento con políticas y reglamentos, la salvaguarda de los activos, el uso económico y eficiente de los recursos, las metas y objetivos operativos establecidos. Los trabajos de auditoría interna

abarcan todas las actividades financieras y de operaciones incluyendo sistemas, producción, ingeniería, comercialización y recursos humanos.

El Instituto de Auditores Internos de los Estados Unidos define la auditoría interna como "una actividad independiente que tiene lugar dentro de la empresa y que está encaminada a la revisión de operaciones contables y de otra naturaleza, con la finalidad de prestar un servicio a la dirección".
Es un control de dirección que tiene por objeto la medida y evaluación de la eficacia de otros controles.

La auditoría interna surge con posterioridad a la auditoría externa por la necesidad de mantener un control permanente y más eficaz dentro de la empresa y de hacer más rápida y eficaz la función del auditor externo. Generalmente, la auditoría interna clásica se ha venido ocupando fundamentalmente del sistema de control interno, es decir, del conjunto de medidas, políticas y procedimientos establecidos en las empresas para proteger el activo, minimizar las posibilidades de fraude, incrementar la eficiencia operativa y optimizar la calidad de la información económico-financiera. Se ha centrado en el terreno administrativo, contable y financiero.

La necesidad de la auditoría interna se pone de manifiesto en una empresa a medida que ésta aumenta en volumen, extensión geográfica y complejidad y hace imposible el control directo de las operaciones por parte de la dirección. Con anterioridad, el control lo ejercía directamente la dirección de la empresa por medio de un permanente contacto con sus mandos intermedios, y hasta con los empleados de la empresa. En la gran empresa moderna esta peculiar forma de ejercer el control ya no es posible hoy día, y de ahí la emergencia de la llamada auditoría interna.

El objetivo principal es ayudar a la dirección en el cumplimiento de sus funciones y responsabilidades, proporcionándole análisis objetivos, evaluaciones, recomendaciones y todo tipo de comentarios pertinentes sobre las operaciones examinadas. Este objetivo se cumple a través de otros más específicos como los siguientes:

a) Verificar la confiabilidad o grado de razonabilidad de la información contable y extracontable, generada en los diferentes niveles de la organización.
b) Vigilar el buen funcionamiento del sistema de control interno (lo cual implica su relevamiento y evaluación), tanto el sistema de control interno contable como el operativo. (Lefcovich)

2.2. Rol de la Auditoría Interna en la Gestión de la empresa (Coso ERM)

Declaración de Posición Nº 1 del I.A.I.

El rol principal de la auditoría interna con respecto a ERM es proporcionar aseguramiento objetivo al consejo de administración respecto de la eficacia de las actividades de ERM de una empresa, para ayudar a garantizar que los riesgos claves del negocio se están gestionando correctamente y que el sistema de control interno está funcionando eficazmente.

2.2.1. Instituto de Auditores Internos (IAI) con relación al rol de Auditoría Interna en la Gestión de Riesgos de la empresa

Los factores principales que los DEA (Directores Ejecutivos de Auditoría) deben tener en cuenta al establecer el rol de la auditoría interna consisten en determinar si la actividad amenaza de alguna manera la independencia y objetividad del auditor interno, y si existe la posibilidad de mejorar los procesos de gestión de riesgos, control y gobierno de la organización. La declaración de posición del IIA indica cuáles son los roles que debe, y que no debe, desempeñar la auditoría interna durante todo el proceso de ERM. (Instituto de Auditores Internos, Rol del Auditor Interno en el ERM.pdf)

2.2.2. Roles fundamentales de la auditoría interna respecto al ERM

- Brindar aseguramiento sobre procesos de gestión de riesgo.
- Brindar aseguramiento de que los riesgos son correctamente evaluados.

- Evaluación de los procesos de gestión de riesgo.
- Evaluación de reporte de riesgos claves.
- Revisión del manejo de los riesgos claves.

2.2.3. Roles legítimos de auditoría interna que deben realizarse con salvaguarda

- Facilitación, identificación y evaluación de riesgos.
- Entrenamiento a la gerencia sobre respuesta a riesgos.
- Coordinación de actividades de ERM.
- Consolidación de reportes sobre riesgos.
- Mantenimiento y desarrollo del marco de ERM.
- Defender el establecimiento del ERM.
- Desarrollo de estrategias de gestión de riesgo para aprobación de la junta.

2.2.4. Roles que auditoría interna NO debe realizar

- Establecer el apetito de riesgo.
- Imponer procesos de gestión de riesgo.
- Manejar el aseguramiento sobre los riesgos.
- Tomar decisiones en respuesta a los riesgos.
- Implementar respuestas a riesgos a favor de la administración.
- Tener responsabilidad de la gestión de riesgo.

El I.A.I. enfatiza que las organizaciones deben entender completamente que la gerencia mantiene la responsabilidad de la gestión de riesgo. Los auditores internos deben proveer consejo, y motivar o soportar las decisiones gerenciales sobre riesgos, en vez de realizar decisiones sobre gestión de riesgo. La naturaleza de las responsabilidades de auditoría interna debe estar documentada en los estatutos de auditoría y ser aprobada por el comité de auditoría.

La auditoría interna, en los roles de aseguramiento y consultoría, contribuye a la gestión de riesgo de formas variadas.

2.2.5. El Rol de la Auditoría Interna en la Gestión de Riesgo Empresarial

Durante los últimos años, la importancia de fortalecer el gobierno corporativo en la gestión de riesgo se ha incrementado notablemente. Las organizaciones están bajo presión para identificar todos los riesgos de negocios que ellas enfrentan; sociales, éticos y ambientales, así como financieros y operacionales, y explicar cómo gestionan los mismos para llevarlos a niveles aceptables. Mientras tanto, el uso de marcos de gestión de riesgo se ha incrementado, debido a que las organizaciones reconocen sus ventajas sobre enfoques menos coordinados de gestión de riesgo.

La auditoría interna, en los roles de aseguramiento y consultoría, contribuye a la gestión de riesgo de formas variadas. En el 2002, el Instituto de Auditores Internos de RU e Irlanda publicó una Declaración de Posición sobre El Rol de la Auditoría Interna en la Gestión de Riesgo, para proveer una guía a sus miembros sobre los roles que están permitidos y las salvaguardas necesarias para proteger la objetividad e independencia de la auditoría interna. Esta nueva declaración de posición sustituye la anterior y toma en cuenta los desarrollos recientes alrededor del mundo en el campo de gestión de riesgo y auditoría interna.

La gente realiza actividades de gestión de riesgo para identificar, evaluar, manejar y controlar toda clase de eventos o situaciones. Estos pueden abarcar proyectos sencillos o tipos de riesgos estrechamente definidos. Por ejemplo: Riesgos de mercado, amenazas y oportunidades que enfrenta la organización como un todo. Los principios presentados en esta declaración de posición pueden usarse como guía en el envolvimiento de auditoría interna en todas las formas de gestión de riesgo, pero nosotros estamos especialmente interesados en la gestión de riesgos, debido a que esta puede mejorar los procesos de gobierno de la organización.

2.2.5.1 Auditoría interna en la función de brindar aseguramiento en el ERM

Uno de los requerimientos claves de la junta o sus equivalentes es obtener aseguramiento de que el proceso de gestión de riesgo está trabajando efectivamente y que los riesgos claves están siendo manejados en niveles aceptables.

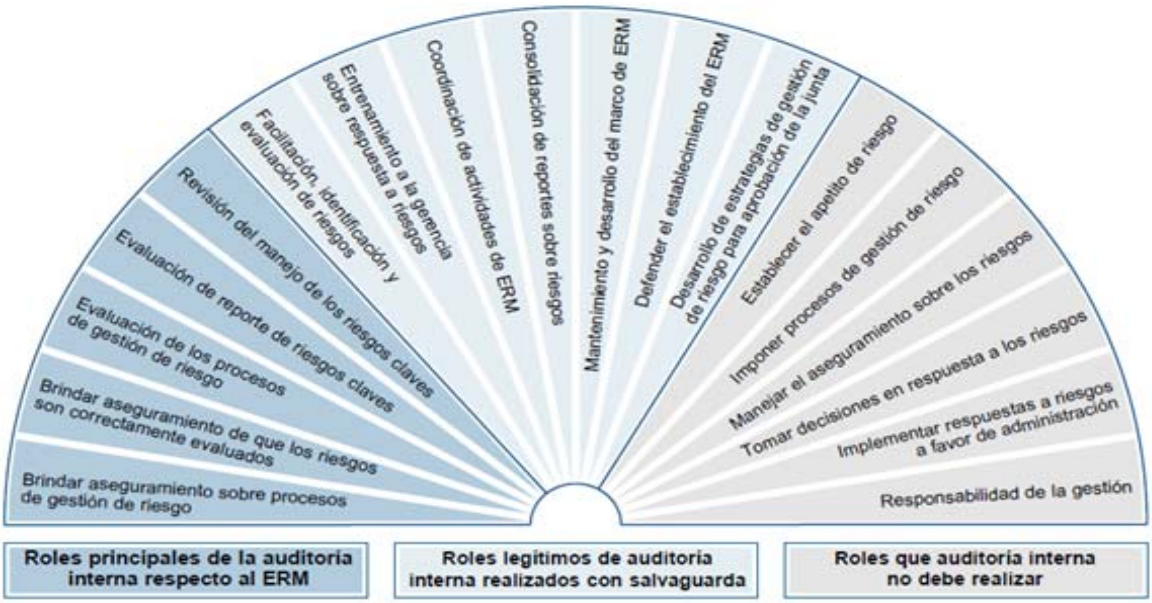
Es posible que el aseguramiento provenga de diferentes fuentes. De estas, el aseguramiento de la gerencia es fundamental. Este debe ser complementado con el proveer aseguramiento de forma objetiva, para lo cual auditoría interna es una fuente clave. Otras fuentes incluyen a los auditores externos y revisiones de especialistas independientes. La Auditoría interna provee aseguramiento normalmente en tres áreas:

- Procesos de gestión de riesgos, tanto en su diseño y como qué tan bien están trabajando;
- Gestión de aquellos riesgos clasificados como "claves", incluyendo efectividad de los controles y otras respuestas a éstos; y
- Confiabilidad y evaluaciones apropiadas de riesgos y reportes de riesgo y estatus de controles.

Brindando aseguramiento - Rol de la auditoría interna en el ERM

La auditoría interna es una actividad independiente, objetiva de aseguramiento y consulta. Su rol principal con relación al ERM es proveer aseguramiento objetivo a la junta sobre la efectividad de la gestión de riesgo.
Igualmente, investigaciones han demostrado que la junta de directores y los auditores internos están de acuerdo que las dos formas más importantes en que la auditoría interna provee valor a la organización es brindando aseguramiento objetivo de que los principales riesgos de negocio están siendo manejados apropiadamente y proveyendo aseguramiento de que la gestión de riesgo y el marco de control interno están operando efectivamente.

La *Figura 18* presenta el rango de las actividades de ERM e indica cuales roles una función de auditoría interna profesional efectiva debe hacer e, igualmente importante que no debe realizar. Los factores claves que deben ser tomados en consideración cuando se determina el rol de auditoría interna son, si la actividad representa alguna amenaza a la independencia y objetividad de la función de auditoría interna, y si podría mejorar los procesos de gestión de riesgo, control y gobierno de la organización.



Roles principales de la Auditoría Interna respecto al ERM	Roles legítimos de Auditoría interna realizados con salvaguarda	Roles que Auditoría Interna no debe realizar
•Brindar aseguramiento sobre procesos de gestión de riesgo. •Brindar aseguramiento de que los riesgos son correctamente evaluados. •Evaluación de los procesos de gestión de riesgo. •Evaluación de reporte de riesgos claves. •Revisión del manejo de los riesgos claves	•Facilitación, identificación y evaluación de riesgos. •Entrenamiento a la gerencia sobre respuesta a riesgos. •Coordinación de actividades de actividades de ERM. •Consolidación de reportes sobre riesgos. •Mantenimiento y desarrollo del marco de ERM. •Defender el establecimiento del ERM. •Desarrollo de estrategias de gestión de riesgo para aprobación de la junta.	•Establecer el apetito de riesgo. •Imponer procesos de gestión de riesgo. •Manejar el aseguramiento sobre los riesgos. •Implementar respuestas a riesgos a favor de administración. •Responsabilidad de la gestión.

Figura 18, Rol de Auditoría Interna en el ERM
Fuente: (Instituto de Auditores Internos, Rol del Auditor Interno en el ERM.pdf)

Las actividades de la izquierda de la *Figura 18* son todas actividades de aseguramiento. Ellas forman parte del objetivo amplio de dar aseguramiento sobre la gestión de riesgo. Una función de auditoría interna cumpliendo con las *Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna* puede y debe realizar por los menos algunas de estas actividades.

La auditoría interna puede proveer servicios de aseguramiento que mejoren los procesos de gobierno, gestión de riesgos y control de la organización. El alcance de la consultoría de auditoría interna en ERM depende de otros recursos, internos y externos, disponibles para la junta y de la madurez del riesgo de la organización y su posibilidad de variar en el tiempo. La experiencia del auditor interno en consideraciones de riesgos, en entendimiento de la conexión entre riesgo y gobierno y en facilitación demuestra que está bien calificado para actuar como defensor y hasta como gerente del proyecto de ERM, especialmente en la etapa inicial de su introducción.

Cuando incrementa la madurez de riesgo en la organización y la gestión de riesgo se encaja más en las operaciones del negocio, el rol de auditoría interna de defensor de ERM se puede reducir. Similarmente, si la organización emplea los servicios de un especialista o posee una función de gestión de riesgo, auditoría interna podría agregar mayor valor a través de concentrarse en su rol de aseguramiento, en vez de realizar mayores actividades de consultoría. Sin embargo, si auditoría interna no ha adoptado todavía el enfoque basado en riesgo representado por las actividades de aseguramiento en la izquierda de la *Figura 18*, no podría estar equipado para realizar las actividades de consultoría.

Rol de Consultoría

El centro de la Figura 18 presenta el rol de consultoría que la auditoría interna puede realizar en relación con el ERM. En general, mientras más a la derecha del cuadro se aventure el auditor, mayores deben de ser las salvaguardadas que son requeridas para asegurarse que la objetividad e independencia son mantenidas. Algunos de los roles de consultoría que auditoría interna puede realizar son:

- Poner a disponibilidad de la gerencia herramientas y técnicas usadas por auditoría interna para analizar riesgos y controles;
- Ser un defensor de la introducción de ERM en la organización, aportando su experiencia en gestión de riesgo y conocimientos de la organización;
- Proveyendo consejo, facilitando talleres, entrenando en la organización sobre riesgos y controles, y promoviendo el desarrollo de un lenguaje, marco y entendimiento común:
- Actuando como punto central de la coordinación, monitoreo y reporte sobre riesgos; y
- Apoyando a la gerencia en su trabajo a través de identificar mejores vías para mitigar un riesgo.

El factor clave en la decisión sobre si los servicios de consultoría son compatibles con el rol de aseguramiento es el determinar si el auditor interno está asumiendo alguna responsabilidad gerencial. En el caso de ERM, la auditoría interna puede proveer servicios de consultoría mientras no tenga rol, actualmente, en la gestión de riesgos esa es una responsabilidad de la gerencia y mientras la alta dirección endose y apoye el ERM. Cada vez que auditoría interna actúe ayudando al equipo gerencial en el establecimiento y mejora de los procesos de gestión de riesgo, su plan de trabajo debe incluir una estrategia clara y un tiempo asignado para transferir la responsabilidad de estas actividades a los miembros del equipo gerencial.

Salvaguardas

La auditoría interna puede ampliar su participación en el ERM, como se muestra en la Figura 18, aplicando ciertas condiciones las cuales son:

- Debe estar claro que la gerencia mantiene la responsabilidad de la gestión de riesgo.
- La naturaleza de la responsabilidad de auditoría interna debe ser documentada en los estatutos de auditoría y aprobado por el Comité de Auditoría.
- Auditoría interna no debe gestionar ningún riesgo en favor de la gerencia.
- Auditoría interna debe proveer consejo, motivar y soportar las decisiones realizadas por la dirección, en vez de tomar decisiones de riesgo por ellos mismos.

- Auditoría interna tampoco puede brindar aseguramiento objetivo en ninguna parte del marco de ERM de la cual es responsable. Tal aseguramiento debe ser provisto por otra parte sustancialmente calificada.
- Cualquier trabajo más allá de las actividades de aseguramiento debe reconocerse como una asignación de consultoría y la implementación de normas relativas a tales asignaciones deben seguirse.

Destrezas y conocimientos

Los auditores internos y gerentes de riesgo comparten algunos conocimientos, destrezas y valores. Ambos, por ejemplo, conocen sobre requerimientos de gobierno corporativo, poseen destrezas de manejo de proyectos, analíticas y de facilitación y tienen valores de crear un balance saludable de riesgo en vez de tomar riesgos extremos o comportamiento evasivo. Sin embargo, los gerentes de riesgo como solamente brindan servicio a la dirección de la organización y no tienen que proveer aseguramiento independiente y objetivo al comité de auditoría.
Tampoco debe el auditor interno que busque ampliar su rol en el ERM subestimar el conocimiento especializado de los gerentes de riesgo (tales como transferencia de riesgo, calificación de riesgos y técnicas de modelos), las cuales están fuera del cuerpo de conocimientos de la mayoría de los auditores internos. Ningún auditor interno que no pueda demostrar las destrezas y conocimientos apropiados debe realizar trabajos en el área de gestión de riesgo. Aún más, la cabeza de auditoría interna no debe proveer servicios de consultoría en esta área si las destrezas y conocimientos dentro de la función de auditoría interna no se encuentran disponibles y no se pueden obtener de otra parte.

La Gestión de riesgo es un elemento fundamental del gobierno corporativo. La gerencia es responsable de establecer y operar el marco de gestión de riesgo con el favor de la junta. La gestión de riesgo brinda muchos beneficios como resultado de su enfoque estructurado, consistente y coordinado. El rol principal de la auditoría interna en relación al ERM debe ser proveer aseguramiento a la dirección y la junta sobre la efectividad de la gestión de riesgo. Cuando la auditoría interna extiende sus actividades más allá de este rol principal,

deben aplicarse ciertas salvaguardas, incluyendo considerar la asignación como servicios de consultoría y, por lo tanto, aplicar todas las normas relevantes. De esta forma, la auditoría interna protege su independencia y objetividad de sus servicios de consultoría. Dentro de estas restricciones, el ERM puede ayudar a subir el perfil e incrementar la efectividad de la auditoría interna.

2.3. Diferencia entre evaluación de Gestión de Riesgos y Auditoría basada en Riesgos.

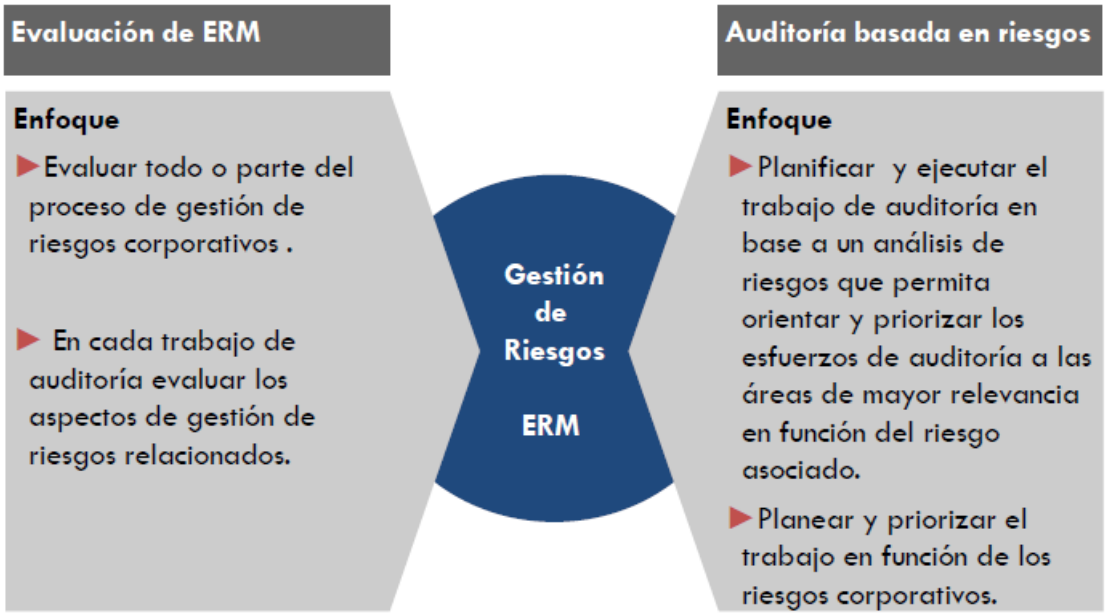


Figura 19, Diferencia entre evaluación de Gestión de Riesgos y Auditoría basada en Riesgos
Fuente: (Badillo, 2010)

La Auditoría basada en Riesgos significa ampliar la perspectiva de la auditoria para incluir todas las técnicas de riesgo, incluyendo técnicas de administración. Esta práctica incluso le proporciona al Auditor una oportunidad para examinar si existe un excesivo control en el proceso de la administración, dándole la oportunidad de señalar e identificar algunos procedimientos que se encuentren obsoletos o sean ineficientes.

Integración con Enterprise Risk Management (ERM) Si bien el Instituto de Auditores Internos (IIA) habla de "auditoría basada en riesgos", muchas organizaciones consideran

que esto significa la identificación de los riesgos de importancia y ponerlos en su plan de auditoría. Pero esto es sólo la mitad de la historia. La verdadera auditoría basada en riesgos integra la auditoría interna con la gestión del riesgo, tanto en la identificación de los riesgos de importancia como en la conducción de la forma y estructura de la respuesta de auditoría. La integración de estas disciplinas (en comparación con las unidades de negocio), provee a la organización con valiosas recomendaciones sobre los riesgos, los controles y los costos.

Auditoría Interna Basada en Riesgos (Risk Based Internal Audit) RBIA

Necesidad de ese enfoque en el sector bancario para la aplicación del Acuerdo de Basilea II: Perspectiva de Bangladesh

RBIA actuará como una herramienta importante al facilitar a la gerencia en el desarrollo de la base de datos de riesgo, que es un documento esencial para cumplir con el Pilar - 1 (requisito de capital mínimo) de Basilea II. Aunque hay algunas dificultades o inconvenientes en la aplicación de RBIA, para pasar a este enfoque es necesario para un beneficio doble:en primer lugar, una mejorada y efectiva forma de conducir la auditoría interna que es requerida para hacer frente a una gran complejidad como resultado del incrementado uso de las tecnologías de la información (TI), requisitos reglamentarios y la globalización en este sentido; y , en segundo lugar, facilitar a la gerencia en el desarrollo y la actualización de la base de datos de riesgos.

2.4. Enfoque de la Auditoría basada en Coso (ERM)

El enfoque de auditoría basada en riesgos contempla las siguientes fases:

1. Comprensión de Objetivos y procesos de negocio relacionados
2. Identificación de Objetivos y Riesgos
3. Evaluación de riesgos
4. Análisis de proceso y riesgo
5. Enfoque de factor riesgo (priorización)

6. Definición del plan.

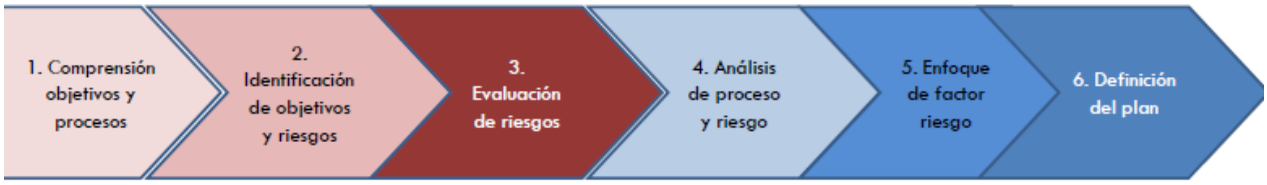


Figura 20, Enfoque de la Auditoría basada en riesgos
Fuente: (Badillo, 2010)

2.4.1. Comprensión de Objetivos y procesos de negocio relacionados.-

Para que los auditores internos puedan agregar valor y mejorar el desempeño de la empresa, primero deben comprender su modelo de negocio. El modelo de negocio incluye los objetivos de la empresa y la forma en que los procesos de negocios estructuran para lograr estos objetivos. Abarca la visión, la misión y los valores, así como también el conjunto de límites de la empresa, es decir, qué productos o servicios entregará, a qué clientes o mercados apuntará y qué canales de suministro y entrega utilizará. Si bien el modelo incluye las estrategias y la dirección táctica sobre cómo la empresa realizará su implementación, también en él se incluyen las metas anuales que establecen los pasos específicos que la empresa adoptará al año siguiente y las medidas correspondientes al logro esperado. (Badillo, 2010)

Existen muchas fuentes con información más detallada acerca de la estrategia de la empresa. Estas son:

- Las declaraciones de visión y misión.
- Los objetivos organizativos estratégicos, operativos, de elaboración de informes y de cumplimiento).
- Las metas anuales de la empresa.
- Las metas anuales de los principales ejecutivos.
- Las presentaciones de planificaciones estratégicas y los documentos relacionados.

Para un auditor interno, o para una persona que no participa directamente en el proceso, la primera fuente de información es la persona a cargo del proceso y la documentación existente sobre políticas y procedimientos relacionados con el proceso. De lo contrario, el auditor deberá trabajar con las principales personas que participaron en el proceso para obtener la información.

- Una vez identificados los objetivos del proceso, el próximo paso es observar los aportes del proceso y las actividades específicas que fueron necesarios para lograr los objetivos (resultados del proceso)

Para lograr una comprensión del proceso es necesario, además de identificar los objetivos clave, comprender cómo la dirección y la persona encargada del proceso saben que el proceso se está realizando como se pretende. La persona encargada del proceso debe establecer los indicadores clave de desempeño (KPI) que se utilizan para supervisar el desempeño del proceso.

Estos indicadores deben ser perceptibles (se pueden medir objetivamente), deben ser relevantes para el objetivo (no se deben utilizar sólo porque se pueden cuantificar), deben estar disponibles de manera oportuna y se deben comunicar a las personas que participaron en el proceso.

La planificación de auditoría basada en riesgos requiere una comprensión integral actualizada del modelo de negocio, esto implica identificar la cadena de valor, los procesos de la organización (mapas de proceso, indicadores KPI) y cómo estos se relacionan entre sí para el logro de objetivos. Adicionalmente esta comprensión requiere comprender aspectos como: visión, misión, valores, estrategias, planes tácticos (metas), productos y / o servicios, clientes, proveedores, reglas y restricciones de negocio.
Este proceso previo a la planificación debería realizarse en circunstancias normales de manera anual. La comprensión del modelo de negocio se puede realizar con alguno de estos enfoques: de arriba hacia abajo (top – down) o de abajo hacia arriba (bottom – up)

Los objetivos pueden ser considerados en las siguientes categorías:

- Estratégicos
- Operaciones (eficientes y efectivas)
- Reportes confiables
- Cumplimiento (normas internas y externas)

Los procesos de negocio deben ser identificados considerando la cadena de valor de la organización. A nivel de macro procesos puede considerarse los siguientes niveles:

- Procesos gobernadores
- Procesos ejecutivos
- Procesos operativos
- Procesos de soporte
-

2.4.2. Identificación de Objetivos y Riesgos

Una vez que se tiene identificados los objetivos de negocio y los procesos clave correspondientes se procede a la identificación de los riesgos que podrían impedir el logro de los objetivos.

La capacidad de comprensión de los riesgos de negocio de parte del auditor interno es fundamental y determinará el grado en que se podrá agregar valor a la organización a través de los trabajos de auditoría interna.
Para cumplir con esta actividad se debe establecer una matriz de Objetivos y Riesgos.

MATRIZ DE OBJETIVOS Y RIESGOS CRÍTICOS Firma de servicios financieros en línea					
Misión: continuar el crecimiento proyectado de entrega de servicios financieros en línea de Norteamérica y reforzar nuestra infraestructura de bajo costo para incrementar la participación en el mercado y la rentabilidad. Mejorar la experiencia del cliente e incrementar el valor para los accionistas.	RIESGOS CRÍTICOS				
	CR1 Económico — Cambios en la dinámica del mercado.	CR2 Estancamiento de producto — Imposibilidad de entregar innovación en productos.	CR3 Disponibilidad — Interrupciones en los sistemas o servicios.	CR4 Continuidad del negocio — Planificación de la continuidad del negocio incompleta.	CR5 Privacidad — Compromiso de privacidad con el cliente.
OBJETIVOS 1. Concentrarse en los servicios para inversores. Concentrarse en captar inversores activos e independientes para nuestros servicios.	X	X	X	X	X
2. Reforzar la infraestructura para agregar ingresos crecientes. Capitalizar nuestra tecnología registrada superior, que permite que los inversores tengan una experiencia en línea excepcional.		X	X	X	X
3. Continuar persiguiendo enérgicamente el crecimiento a través de las adquisiciones.	X	X			
4. Reforzar nuestra sólida marca.	X	X			
5. Continuar ofreciendo tecnologías innovadoras y mejoras de servicio a nuestros clientes.	X	X	X	X	X

Figura 21, Matriz de Objetivos y Riesgos Críticos

Fuente: (Badillo, 2010)

2.4.3. Evaluación de riesgos

Una vez que el auditor interno logra una comprensión de los objetivos de la empresa y de los procesos clave utilizados para lograr esos objetivos, debe evaluar los riesgos del negocio que podrían impedir el logro de los objetivos. La capacidad del director ejecutivo de auditoría (DEA) y de la dirección de auditoría interna para lograr una comprensión cabal

de los riesgos de negocio de la empresa determinará el grado hasta el cual la función de auditoría interna podrá cumplir con su misión y agregar valor a la empresa.

La evaluación de riesgos se debe hacer considerando y validando lo generado por el área de gestión de riesgos si esta existe y dependiendo de su nivel de madurez, el auditor deberá complementar en la medida de lo necesario la evaluación de riesgos para fines de su plan de auditoría.

2.4.4. Análisis de proceso y riesgo

Para seleccionar correctamente las estrategias de respuesta adecuadas, es necesario comprender cómo el riesgo se relaciona con los procesos de negocio de la empresa. Los auditores internos también deben establecer el vínculo entre el riesgo y el proceso de negocio para determinar si el riesgo se está gestionando o no en el nivel adecuado dentro de la estrategia de respuesta de la gestión y para identificar en qué área de la empresa reside el riesgo crítico. Recuerde que la Norma 2010 requiere explícitamente que el DEA "establezca planes basados en riesgos para determinar las prioridades de la actividad de auditoría interna, en conformidad con las metas de la empresa". (Badillo, 2010)

Una vez evaluados los riesgos se debe asociarlos a los procesos respectivos identificando si existen una vinculación clave o una vinculación secundaria. Una vinculación clave entre un proceso y un riesgo se presenta cuando existe una relación directa y principal.

2.4.5. Enfoque de factor riesgo (priorización)

Otro enfoque más indirecto de la vinculación de procesos de negocio y riesgos se realiza a través del desarrollo de factores de riesgo básicos utilizados para evaluar los riesgos en los procesos (enfoque de factor de riesgo). Por lo general, los modelos de factor de riesgo identifican de 7 a 15 factores que se pueden utilizar para evaluar cada proceso.

Son de un mayor nivel de abstracción, que se puede aplicar a cada proceso. La mayoría de los modelos están compuestos por dos tipos de factores básicos factores de riesgo externo y factores de riesgo interno. Los factores de riesgo externo se relacionan con factores creados en el entorno y la naturaleza del proceso mismo.

Una vez que se cuenta con la matriz de proceso riesgo se puede emprender en la determinación priorizada de los procesos a incorporarse en el plan de auditoría y los ciclos de revisión.

- La primera priorización puede realizarse en función del número de vinculaciones clave y secundarias de cada proceso. Esto permitirá establecer un ciclo de auditoría para aquellos procesos con mayores vinculaciones clave con los riesgos críticos o moderados (ciclos de uno o dos años) y para los que solamente poseen vinculaciones secundarias (ciclos de tres o cuatro años).

- Adicionalmente, a las consideraciones de vinculaciones clave o secundarias se puede aplicar un enfoque de factor de riesgo considerando aspectos como los siguientes:
  - Factores de riesgo externo: activos en riesgo, visibilidad, complejidad, tamaño del proceso / operación, requisitos legales.
  - Factores de riesgo interno: estabilidad del control interno, eficacia del control interno, cambios.

Es importante tener en cuenta que, independientemente de la escala seleccionada (una escala de tres, cinco, siete o X puntos), se debe utilizar la misma escala para la evaluación de todos los factores.

- Luego, se debe tomar una decisión sobre la importancia relativa (o peso) de un factor respecto de otro. Si todos los factores de riesgo son considerados de igual importancia, se les debería asignar la misma importancia numérica. Por lo general, la importancia se establece asignando números del O al 100, de manera que la suma de los puntajes de importancia sea igual a 100. Entonces, si tuviéramos cinco factores de riesgo y todos los

factores fueran considerados de igual importancia, a cada factor se le asignaría una importancia de 20. En el modelo de factor de riesgo mostrado al factor estabilidad de control interno se le asigna una importancia de 5, lo que significa que su importancia sólo equivale a la mitad de la importancia del factor Activos en riesgo y a un tercio de la correspondiente al factor Cambios importantes.

La decisión final consiste en cómo se combinan los factores de riesgo. La mayoría de los enfoques de factor de riesgo utilizan un modelo de adición ponderada, en el que el puntaje de cada factor se multiplica por la importancia del factor y se suman todos los factores para obtener un puntaje total de riesgos. Los puntajes totales pueden ser de 100 a 300 y se pueda interpretar como de riesgo bajo (puntajes inferiores a150), riesgo medio (puntajes de 150 a 239) y riesgo alto (puntajes superiores a 240). Una vez determinada la distribución de puntajes en todos los procesos, se deben ajustar los puntajes de limitación de cada categoría. Las categorías se pueden utilizar para asignarle al proceso un ciclo de auditoría de uno, dos, tres o cuatro años. Además, si a un proceso se le asigna un ciclo de dos años, se podría programar para ser auditado cada dos años. (Instituto de Auditores Internos, Auditoría Interna: Servicios de aseguramiento y consultoría)

ENFOQUE DE FACTOR DE RIESGO Descripción y escalas de factores		
Descripción del factor de riesgo		
Factores del riesgo externos	**Puntaje del factor**	**Explicación**
1. Activos en riesgo.	1 2 3	Menos de $500.000 Más de $500.000, menos de $5 millones. Más de $5 millones.
2. Visibilidad.	1 2 3	Unidad operativa/cliente directo. Divisional/grupo limitado de clientes. Empresa/prensa nacional.
3. Complexity.	1 2 3	Tareas simples no calificadas forman el proceso. Requiere varios pasos y la interacción de varias personas. Varios pasos que requieren coordinación de varias personas dentro del proceso y con otros procesos.
4. Tamaño del proceso/ operación.	1 2 3	El proceso afecta a menos del 3% de las actividades de la empresa. El proceso afecta del 3% al 15% de las actividades de la empresa. El proceso afecta a más del 15% de las actividades de la empresa.
5. Requisitos legales/ reglamentarios externos.	1 2 3	Pocos requisitos, no regulados. Algunos requisitos reglamentarios. Una cantidad importante de requisitos complejos.
Factores de riesgo internos	**Puntaje del factor**	**Explicación**
6. Estabilidad del control interno (CI).	1 2 3	Sistema de control y vencimientos de riesgos. Sistema de control y cumplimiento estable. Enfoque ad hoc hacia el control y el cumplimiento.
7. Eficacia del control interno.	1 2 3	Sin problemas de CI o cumplimiento en los últimos dos años. Varios casos de fraude, debilidad del CI o fallas en el cumplimiento pero no de gran importancia en los últimos dos años. Fraude, debilidades de CI o fallas en el cumplimiento de gran importancia en los últimos dos años.
8. Cambios importantes en las operaciones, procesos, personal o tecnología del negocio.	1 2 3	Sin cambios importantes en los últimos 12 meses. Algunos cambios en el proceso o en el personal clave en los últimos 12 meses. Cambio importante en el negocio y en el proceso o nuevo sistema de TI en los últimos 12 meses.
Otros factores	**Puntaje del factor**	**Explicación**
9. Estado o preocupación de la dirección.	1 2 3	Sin preocupaciones. Algunas preocupaciones expresadas por la alta dirección. Preocupación considerable expresada por la alta dirección o el consejo.
10. Resultados de auditorías anteriores.	1 2 3	Sin problemas de control o cumplimiento en la última auditoría. Problemas menores de control o cumplimiento en la última auditoría. Debilidades importantes en el CI en la última auditoría.

Figura 22, Esquema de enfoque de factor riesgo

Fuente: (Badillo, 2010)

IMPORTANCIA Y PUNTAJE DEL ENFOQUE DE FACTOR DE RIESGO				
Factor de riesgo				
Factores de riesgo externo	Puntaje	Importancia X	Puntaje ponderado	
1. Activos en riesgo		10		
2. Visibilidad		10		
3. Complexity.		10		
4. Tamaño del proceso/operación.		10		
5. Requisitos legales/reglamentarios externos.		10		
Puntaje del riesgo externo total				
Internal Risk Factors	Puntaje	Importancia X	Puntaje ponderado	
6. Estabilidad del control interno (CI).		5		
7. Eficacia del control interno.		10		
8. Cambios importantes en las operaciones, procesos, personal o tecnología del negocio.		15		
Puntaje del riesgo interno total				
Otros factores	Puntaje	Importancia X	Puntaje ponderado	
9. Estado o preocupación de la dirección.		10		
10. Resultados de auditorías anteriores.		10		
Puntaje total de otros riesgos				
Puntaje total de riesgos				

Figura 23, Importancia y puntaje del factor riesgo

Fuente: (Badillo, 2010)

2.4.6. Definición del plan.

Para definir el plan de auditoría se considera:

- El análisis de vinculaciones clave y secundarias entre procesos y riesgos.
- La aplicación del enfoque de factor de riesgo.
- Adicionalmente se puede aplicar los aspectos antes mencionados de una clasificación de los procesos que serían sujetos de auditoría.
- Finalmente la definición de los procesos a ser auditados y los ciclos de auditoría respectivos comprenden el eje del Plan de Auditoría, posteriormente se debe realizar la estimación y asignación de recursos y proceder a la ejecución del plan.

- Los planes de auditoría basados en riesgos deberían ser actualizados anualmente pues es el mismo período en que usualmente se actualiza la gestión de riesgos. Esto salvo circunstancias especiales o extraordinarias.

ENFOQUE DE FACTOR DE RIESGO
Análisis de riesgo por proceso de negocio

	Externos	Internos	Otros
Proceso 1			
Proceso 2			
Proceso 3			
Proceso 4			
Proceso 5			
Proceso 6			
Proceso 7			
Proceso 8			
Proceso 9			
Proceso 10			
Proceso 11			
...			
Proceso n			
Nivel de riesgo	**Externos**	**Internos**	**Otros**
Rango potencial de puntajes	50 a 150	30 a 90	20 a 60
Bajo	<90	<50	<35
Medio	90-124	50-74	35-49
Alto	>125	>75	>50

Figura 24, Esquema para definición de procesos a auditarse y los ciclos correspondientes
Fuente: (Badillo, 2010)

Principios fundamentales del plan de auditoría interna basada en riesgos

- La auditoría se debe basar fundamentalmente en el riesgo.
- Se debe considerar los riesgos, inherentes claves, para una auditoría más profunda y frecuente.
- El objetivo fundamental es mitigar los riesgos de todas las áreas del negocio, por lo menos una vez cada 3 años.
- La naturaleza y extensión de los procedimientos reflejarán las necesidades de aseguramiento para la mitigación de riesgos, y tomará en cuenta otras fuent4es como la del comité de auditoría, la gerencia y dirección de las compañías.

- El plan de auditoría será preparado en conjunto por los departamentos involucrados. Dicho plan debe ser flexible a los cambios de acuerdo a las necesidades de información, identificación y mitigación de riesgos.
- Los cambios efectuados al plan de auditoría deberán ser revisados, aprobados y deberán tener la adecuada supervisión del comité de Auditoría. (Yánez, 2014)

Según la normativa de los entes de control JB-2010-1549 un plan debe contener al menos lo siguiente:

"ARTÍCULO 10.- En el plan anual de trabajo de auditoría interna, deberán incluirse todas las labores a desarrollarse.
Dicho plan deberá ser aprobado por el directorio u organismo que haga sus veces.
10.1 Objetivos y alcance del plan, fundamentando las prioridades del mismo;
10.2 Actividades, exámenes e informes y cronograma de los mismos;
10.3 Recursos humanos disponibles para el cumplimiento del plan, indicando de ser el caso la necesidad de contratación de servicios especializados; y,
10.4 Seguimiento a las observaciones formuladas por la Superintendencia de Bancos y Seguros". (Superintendencia de Bancos y Seguros de la República del Ecuador, 2005)

2.5. Lineamientos para realizar una Auditoría Basada en Riesgos

El marco para la práctica profesional de la auditoría interna del IAI contempla aspectos relacionados con la ABR en los siguientes lineamientos:

- Consejo para la Práctica 2010-1: Enlace del Plan de Auditoría con los Riesgos y Exposiciones.
- Practice Advisory 2010-2: Using the Risk Management Process in Internal Audit Planning
- Practice Advisory 2050-2: Assurance Maps
- Consejo para la Práctica 2120-1: Evaluar la Adecuación de los Procesos de Gestión de Riesgos.

- Practice Advisory 2120-2: Managing the Risk of the Internal Audit Activity
- Consejo para la Práctica 2200-1: Planificación del Trabajo
- Consejo para la Práctica 2210-1: Objetivos del Trabajo
- Consejo para la Práctica 2210.A1-1: Evaluación de Riesgos en la Planificación del Trabajo.

Norma principalmente relacionada

2010 –Planificación

- El director ejecutivo de auditoría debe establecer planes basados en los riesgos, a fin de determinar las prioridades de la actividad de auditoría interna. Dichos planes deberán ser consistentes con las metas de la organización. (España, 2011)

Interpretación:

- El director ejecutivo de auditoría es responsable de desarrollar un plan basado en riesgos. Para ello, debe tener en cuenta el enfoque de gestión de riesgos de la organización, incluyendo los niveles de aceptación de riesgos establecidos por la dirección para las diferentes actividades o partes de la organización. Si no existe tal enfoque, el director ejecutivo de auditoría utilizará su propio juicio sobre los riesgos después de consultar con la alta dirección y el Consejo.
-

Consejo para la práctica 2010-1:

Enlace del Plan de Auditoría con los riesgos y exposiciones

1. Al elaborar el plan de auditoría interna, muchos directores ejecutivos de auditoría (DEAs) consideran útil, en primer término, elaborar o actualizar el universo de auditoría. El universo de auditoría es una lista de todas las auditorías posibles que pudieran realizarse. El DEA puede obtener información sobre el universo de auditoría de parte de la alta dirección y el consejo de administración.

2. El universo de auditoría puede incluir componentes del plan estratégico de la organización. Al incorporar esos componentes, el universo de auditoría considerará y reflejará los objetivos del plan general de negocios. Los planes estratégicos probablemente también reflejarán la actitud de la organización hacia el riesgo y el grado de dificultad para cumplir con los objetivos planificados. El universo de auditoría estará normalmente influenciado por los resultados del proceso de gestión de riesgos. **El plan estratégico de la organización tiene en cuenta el ambiente en el cual opera la organización**. Estos mismos factores ambientales probablemente impactarán en el universo de auditoría y la evaluación del riesgo relativo.

3. El DEA prepara el plan de auditoría de la actividad de auditoría interna basándose en el universo de auditoría, informaciones recibidas de la alta dirección y el consejo de administración, y una evaluación de riesgos y exposiciones que afectan a la organización. Los objetivos clave de auditoría son usualmente los que proporcionará la alta dirección y al consejo de administración aseguramiento e información que les permita cumplir con los objetivos de la organización, incluyendo una evaluación de la eficacia de las tareas de evaluación de riesgos que realiza la dirección.

4. El universo de auditoría y el plan de auditoría relacionado se mantienen actualizados de modo de reflejar los cambios en la dirección de la gestión, objetivos, énfasis y enfoques. **Es aconsejable evaluar el universo de auditoría al menos una vez al año con el fin de que refleje las estrategias y la dirección más actualizadas de la organización.** En algunas situaciones, los planes de auditoría pueden tener que actualizarse más frecuentemente (por ejemplo, trimestralmente), en respuesta a los cambios en los negocios, operaciones, programas, sistemas y controles de la organización.

5. El calendario de trabajo de auditoría está basado, entre otros factores, en una evaluación de riesgos y exposiciones. Establecer prioridades es necesario para tomar decisiones asignar los recursos relativos. Existe una variedad de modelos de riesgo para ayudar al DEA. La mayoría de los modelos de riesgo utilizan factores de riesgo tales como:

impacto, probabilidad, materialidad, liquidez de activos, competencia de la gerencia, calidad de los controles internos y adhesión a los mismos, grado de cambio o estabilidad, tiempo transcurrido desde la última auditoría y sus resultados, complejidad, y relaciones con el personal y el gobierno.

Existen Normas relacionadas con la Auditoría Interna que dan los lineamientos para realizar una Auditoría basada en Riesgos y son los siguientes:

a) **Norma Relacionada - 2010-Planificación**

El director ejecutivo de auditoría debe establecer planes de riesgo basado para determinar las prioridades de la actividad de auditoría interna, en consonancia con los objetivos de la organización.

b) Norma principalmente relacionada

2200 - Planificación del trabajo

Los auditores internos deben elaborar y documentar un plan para cada trabajo, que incluya su alcance, objetivos, tiempo y asignación de recursos.

c) Consejo para la Práctica 2210-1: Objetivos del Trabajo

2210. A1 - Los auditores internos deben realizar una evaluación preliminar de los riesgos relevantes para la actividad bajo revisión. Los objetivos del trabajo deben reflejar los resultados de esta evaluación.

d) Consejo para la Práctica 2210-1: Objetivos del Trabajo

Norma principalmente relacionada - 2210 - Objetivos del trabajo

Deben establecerse objetivos para cada trabajo.

- Los auditores internos establecen los objetivos del trabajo con el fin de revisar los riesgos asociados con la actividad bajo revisión. Para los trabajos planificados, los objetivos provienen y están alineados con aquellos inicialmente identificados

durante el proceso de evaluación de riesgos del cual se deriva el plan anual de auditoría. Para los trabajos no planificados, los objetivos se establecen antes del comienzo de cada trabajo y están diseñados para revisar el problema específico que motivó la realización de cada abajo.

- La evaluación de riesgos que se realiza durante la fase de planificación del trabajo se utiliza para definir más adelante los objetivos iniciales e identificar las áreas significativas de problemas.

- Una vez identificados los riesgos, el auditor determina los procedimientos a realizar y el alcance (naturaleza, tiempo y extensión) de aquellos procedimientos. Los procedimientos del trabajo llevados a cabo con el alcance apropiado son el medio que permitirá sacar conclusiones referidas a los objetivos del trabajo.

e) Consejo para la Práctica 2210.A1-1: Evaluación de Riesgos en la Planificación del Trabajo

Los auditores internos tienen en cuenta la evaluación de riesgos realizada por la dirección que sea relevante para la actividad bajo revisión. El auditor interno también contempla lo siguiente:

- La fiabilidad de la evaluación de riesgos realizada por la dirección.
- El proceso que sigue la dirección para vigilar, informar y resolver asuntos de riesgos y control.
- Los informes de la dirección sobre eventos que hayan excedido los límites de la organización respecto de la aceptación de riesgos y la respuesta de la dirección a aquellos informes.
- Los riesgos en actividades relacionadas que sean relevantes para la actividad bajo revisión.

Cuando corresponda, los auditores internos realizan un estudio para familiarizarse con las actividades, riesgos y controles, con el fin de identificar las áreas en las que se

deberá poner más énfasis en el trabajo y lograr comentarios y sugerencias de parte de los clientes del trabajo.

Los auditores internos resumen los resultados a partir de las revisiones de la evaluación de riesgos realizada por la dirección, la información de antecedentes, y cualquier estudio llevado a cabo. Este resumen incluye:

- Temas significativos del trabajo y las razones para seguirlos con mayor profundidad.
- Objetivos y procedimientos del trabajo.
- Metodologías a utilizar, tales como auditoría basada en tecnología y técnicas de muestreo.
- Posibles puntos de control críticos, deficiencias de control o exceso de controles.
- Cuando corresponda, las razones para no proseguir el trabajo o para modificar significativamente los objetivos del trabajo. (España, 2011)

2.6. Lineamientos del Coso ERM – Auditoría Basada en Riesgos

Para las Auditorías basada en Riesgos, se debe trabajar el riesgo desde sus diferentes ópticas como el quehacer cotidiano porque forma parte del proceso metodológico es importante enfatizar que este proceso no es individualizado sino compartido con los auditados en otras palabras el enriquecimiento del proceso se obtiene cuando se comparte los análisis y conclusiones con los dueños o responsables de los procesos auditados como:

Planeación:

Todos los trabajos que proyecte el auditor se deben establecer con planes basados en los riesgos, a fin de determinar las prioridades de la actividad de auditoría interna. Dichos planes deben ser consistentes con las metas de la organización, y estarán basados en una evaluación de riesgos, realizada al menos anualmente. En este proceso deben tenerse en cuenta los comentarios de la alta dirección.

Una herramienta empleada en la planeación consiste en una matriz en donde al nivel de las columnas se relacionan los factores de riesgo y a nivel de las filas los procesos auditables, esta metodología permite compararlos bajo una misma base de factores de riesgos, como impacto económico, sanciones legales, afectación a clientes (internos y externos).
La principal ventaja de trabajar la planeación con base en los riesgos es que las auditorías se priorizan con base en las situaciones de riesgo del negocio y sirven posteriormente en la construcción de los mapas de riesgo con los auditados.

Evaluación de riesgos y controles

Es una fase en la que el auditor y el auditado aprovechan la sinergia al unir los conocimientos técnicos del auditor con la experiencia y conocimiento de los auditados al nivel de los riesgos de los procesos del negocio, las causas que los originan, los efectos o riesgos resultantes y los controles existentes para mitigarlos, o en su defecto la propuesta de nuevos controles que eviten o mitiguen los efectos negativos de los riesgos.
La naturaleza del trabajo del auditor interno esta en evaluar y contribuir a la mejora de los sistemas de gestión de riesgos, control y gobierno, asistiendo a la organización en la identificación y evaluación de las exposiciones significativas a los riesgos, y la contribución a la mejora de los sistemas de gestión de riesgos.
Las exposiciones al riesgo referidas a gobierno, operaciones y sistemas de información con relación a lo siguiente:

- Confiabilidad e integridad de la información financiera y operativa.
- Eficacia y eficiencias de las operaciones.
- Protección de activos.
- Cumplimiento de leyes, regulaciones y contratos.

Enfoque de factor riesgo según la planificación ABR

- La primera priorización puede realizarse en función del número de vinculaciones clave y secundarias de cada proceso. Esto permitirá establecer un ciclo de auditoría para

aquellos procesos con mayores vinculaciones clave con los riesgos críticos o moderados (ciclos de uno o dos años) y para los que solamente poseen vinculaciones secundarias (ciclos de tres o cuatro años).

Metodología para la administración integral de los riesgos

La administración del riesgo es un término aplicado a un método lógico y sistemático que establece el contexto, identificación, análisis, evaluación, tratamiento, monitoreo y comunicación sobre los riesgos asociados con una determinada actividad, función o proceso, con el fin de capacitar a las organizaciones para minimizar sus pérdidas y maximizar sus oportunidades.

Una vez adquirido el conocimiento del manejo de los riesgos se describen las etapas necesarias para administrar en forma integral los riesgos del negocio ERM, mediante la gestión y direccionamiento de los Auditores Internos.
Es importante tener en cuenta antes de entrar a la metodología ERM, es importante tener en cuenta los siguientes aspectos para evitar que por su inexistencia o incumplimiento el manejo integral del riesgo falle en la empresa.

Apoyo de la Administración:
Se debe contar con el apoyo total e incondicional de la alta dirección esto con el fin de evitar la creación de áreas independientes o de ideas contrarias.

Objetivos Claros:
Es importante que se especifiquen las responsabilidades de cada integrante en relación con la Administración de riesgos, para evitar suspicacias o errores de interpretación.

Cronogramas:
Los mejores métodos de supervisión y seguimiento por parte del auditor al manejo de la administración de riesgos en cuanto a las fases, responsabilidades, tiempos, entregables,

verificaciones, compromisos e indicadores se puede apoyar el auditor con cronogramas elaborados en un manejador de proyectos.

Recursos:

No solo el tiempo del desarrollo de los talleres es importante para obtener buenos resultados, pues hay que disponer de los recursos financieros, físicos y tecnológicos para el desarrollo de los talleres y la consolidación de la información.

Formación de equipos:

Para que la metodología de administración de riesgos funcione ésta debe ser respaldada por equipos integrados por los dueños o responsables de los procesos, facilitados u orientados por los auditores internos, quienes se acompañarán de herramientas y metodologías que faciliten el desarrollo y análisis de los riesgos.

Metodologías:

Permiten afinar los procesos de trabajo, evitan que cada unidad de negocio vaya por su lado, estandarizan y normalizan las actividades que se deben ir ejecutando y documentando.

Las metodologías son la esencia de cualquier cambio porque marcan los pasos a seguir, estas deben estar documentadas (papel o mejor en medio magnético, intranet) y actualizadas, como: metodologías de auditoría basada en riesgos; metodología de análisis de información cualitativa y cuantitativa como CSA Control Self Assessment o Autocontrol; metodología para el análisis y mejoramiento de procesos; metodología de la auditoría al seguimiento y cumplimiento de los planes de acción de eliminación de causas de riesgo.

Herramientas:

Corresponde a todos aquellos archivos en medio electrónicos estructurados en la hoja electrónica Excel que permite a unos bajos costos y amigabilidad en su ejecución poder desarrollar las metodologías:

- Matrices de auditoría basada en riesgos

- Mapa de riesgos
- Documentación del proceso de priorización y tratamiento
- Glosario de términos con ejemplos de su significado

Bases de datos:

Son los archivos donde se deja toda la información sobre los riesgos, sus categorías, planes de acción, de mitigación y control, responsables, mapas de riesgo y cronogramas que faciliten el análisis y supervisión del auditor en el cumplimiento de la metodología.

Política de administración de riesgo

La organización o entidad debe definir y documentar las políticas de administración del riesgo, incluyendo sus objetivos y su compromiso para ello esta política debe ser importante dentro del contexto estratégico de la empresa, sus objetivos y metas, y la naturaleza del negocio. La alta gerencia debe asegurarse que esta política es entendida, implantada y mantenida por todos los niveles de la organización.

2.7. Diagnóstico Foda

Las fortalezas y debilidades.- son características predominantes internas en las organizaciones. Es necesario reconocer las fortalezas sobre las cuales acumular éxitos y reconocer las debilidades para poder remediarlas.

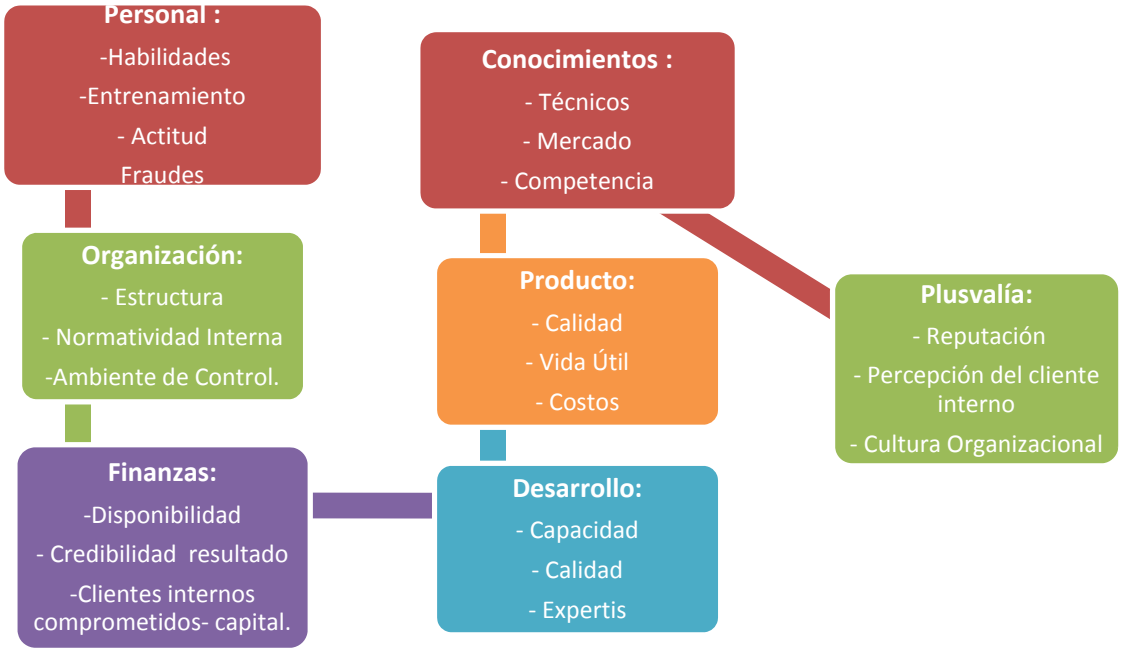


Figura 25: Fortalezas y Debilidades del ABR según Coso ERM

Fuente: (Cuadrado Andrea, 2014)

Oportunidades y Amenazas.- Las circunstancias pueden presentar oportunidades o amenazas a una organización, dependiendo de la capacidad de ésta para explotar. Las oportunidades deben reconocerse y tomar medidas para manejarlas. De no realizarlas la organización puede sufrir graves consecuencias.

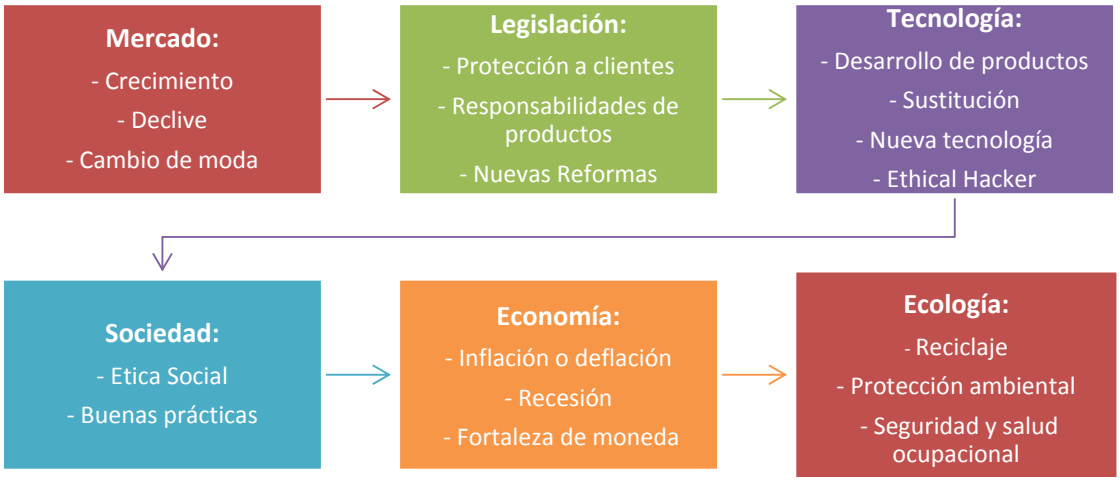


Figura 26: Oportunidades y amenazas del ABR según Coso ERM

Fuente: (Cuadrado Andrea, 2014)

3. EVALUACIÓN DE LA METODOLOGÍA ABR (AUDITORÍA BASADA EN RIESGOS) SEGÚN COSO ERM

Evolución de la Auditoría Basada en Riesgos

La función de auditoría interna ha evolucionado conforme los requerimientos organizacionales se han especializado durante el tiempo, desde: revisiones en las cuales el criterio profesional del auditor incidía totalmente; el establecimiento de programas de trabajo; evaluación del control interno; consideraciones de un modelo de seguridad de auditoría; hasta concluir con el enfoque más moderno e integral: la auditoría basada en riesgos, que considera objetivos, riesgos y controles de negocio, y el riesgo de auditoría.

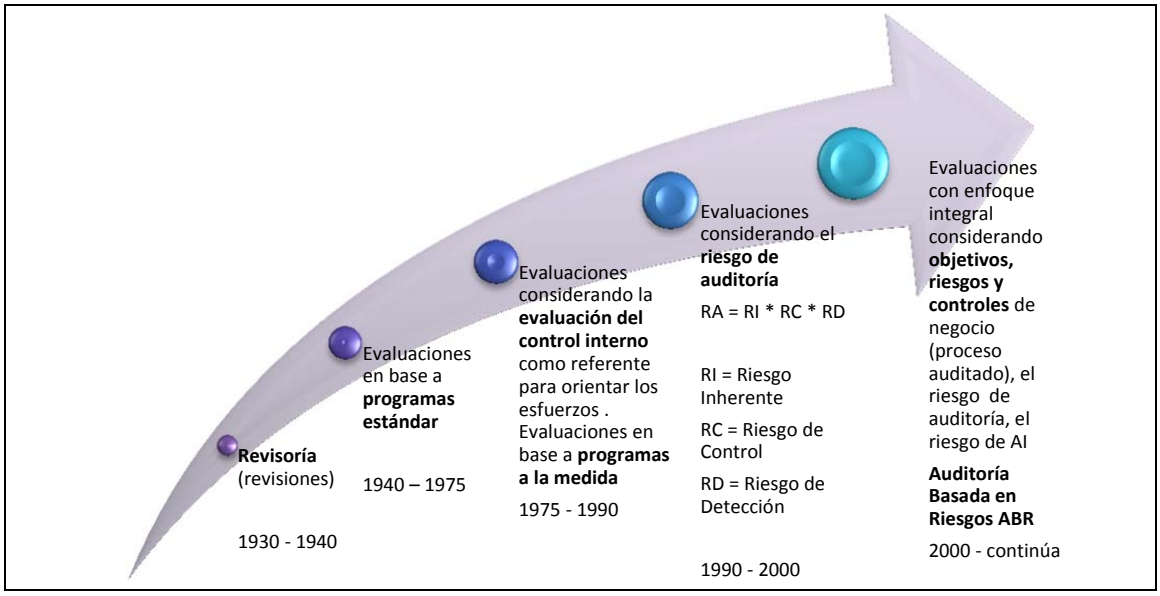


Figura 27, Evolución de Auditoría Basada en Riesgos

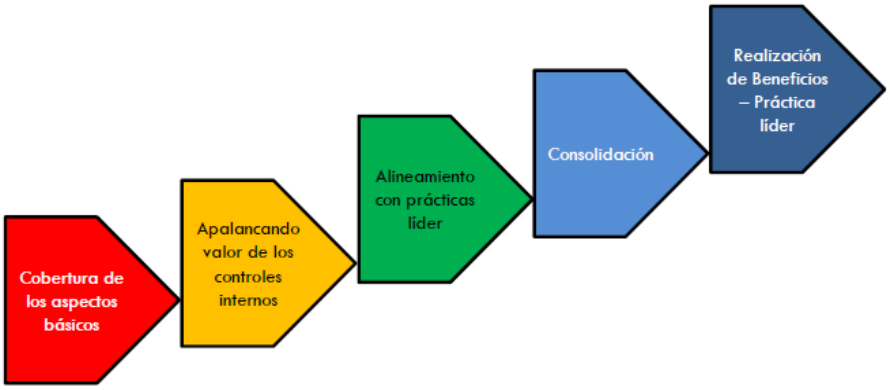
Fuente: (Badillo, 2010)

El enfoque de auditoría interna actualmente se basa en la aportación de valor a la dirección, a través de la relación entre objetivos estratégicos de la organización y la gestión de riesgos del negocio. Los objetivos estratégicos y los riesgos de negocio, junto con las exigencias normativas, deben constituir la base de la actividad de la auditoría interna.

La auditoría basada en riesgos, integra la auditoría interna con la gestión del riesgo, tanto en la identificación de los riesgos de importancia como en la conducción de la forma y estructura de la respuesta de auditoría. La integración de estas disciplinas provee a la organización valiosas recomendaciones sobre riesgos, controles y costos.

Un enfoque no consiste en una sola política sino en una selección de componentes que pertenecen a una organización y que trabajan conjuntamente para gestionar el riesgo de forma eficaz y eficiente a través del tiempo. Es tarea del auditor evaluar si la suma de estos componentes conforma un enfoque adecuado para la organización.

Evolución del enfoque de la Actividad de Auditoría Interna



Proporción del enfoque de auditoria

Controles Financieros	70%	66%	40%	20%	10%
Riesgos Clave	20%	33%	55%	70%	80%
Ad-Hoc	10%	1%	5%	10%	10%

Figura 28, Evolución del enfoque de la Actividad de Auditoría Interna

Fuente: (Badillo, 2010)

La adopción de un enfoque de auditoría depende en gran proporción del estado de madurez de dicha función en una entidad, como se aprecia en el gráfico anterior, se conjugan tres estilos de auditoría: controles financieros, riesgos clave y ad-hoc; en los cuales estos se complementan; dependiendo del estado de madurez de la función de auditoría, uno u otro es el que prevalece. El enfoque de auditoría basada en riesgos, empieza a tomar fuerza en la etapa de "alineamiento de prácticas líder" y cobra importancia mayoritaria en la

“consolidación” y “realización de beneficios-prácticas líder”, en las cuales, su participación puede llegar hasta el 80% del enfoque de trabajo.
Los recursos de auditoría interna se orientan generalmente a las áreas de mayor riesgo, por lo que, el enfoque se debe auditar periódicamente para asegurar que este permite identificar los riesgos adecuadamente y de esta manera, asignar recursos, planificar la auditoría y tomar otras decisiones.

Los auditores deben prestar atención a las actitudes y los valores expresados en relación con la gestión de riesgos en las políticas de la organización, el marco de gobierno y el conjunto de procesos y herramientas de gestión de riesgos. A pesar de que los auditores no participan en el establecimiento del enfoque (el cual debe ser diseñado por la empresa misma), cuando llevan a cabo una auditoría, están evaluando los elementos del enfoque de la organización.

Requerimientos Normativos y Técnicos

La aplicación de la Auditoría Basada en Riesgos responde a requerimientos, profesionales establecidos por el Instituto de Auditores Internos – IAI, normativos exigidos por la Superintendencia de Bancos y Seguros del Ecuador y prácticas del Comité de Basilea.
A continuación incluimos un extracto de los requerimientos mencionados:

Resolución de la Junta Bancaria No. JB-2010-1549, del 21 de enero de 2010

En el artículo 8, incluir como incisos finales, los siguientes:
“La auditoría basada en riesgos consiste en un conjunto de procesos mediante los cuales la auditoría provee aseguramiento independiente al directorio u organismo que haga sus veces, acerca de:

8.1 Si los procesos y medidas de gestión del riesgo que se encuentran implementadas están funcionando de acuerdo a lo esperado;
8.2 Si los procesos de gestión de riesgos son apropiados y están bien diseñados; y,

8.3 Si las medidas de control de riesgos que la gerencia ha implementado son adecuadas y efectivas, y reducen el riesgo al nivel de tolerancia aceptado por el directorio u organismo que haga sus veces.

La auditoría basada en riesgos depende del nivel de desarrollo que la propia institución del sistema financiero ha alcanzado en la gestión de riesgos en el área objeto de examen, y el grado en que han sido definidos objetivos determinados por la gerencia contra los cuales pueden medirse los riesgos asociados.

Cuando la institución del sistema financiero cuenta con un sistema de gestión del riesgo adecuado en las área bajo examen, sin perjuicio de la necesidad de verificaciones adicionales propias del debido cuidado profesional, la auditoría basada en riesgos puede confiar en mayor grado en la evaluación del riesgo que la propia institución ha realizado, y desarrollar un plan basado en riesgos que complemente las acciones realizadas por la entidad y aumente el valor de las actividades de la auditoría interna y mejor e introduzca como una práctica la cultura del control interno basado en estos elementos.

Cuando la institución del sistema financiero cuenta con un sistema de gestión de riesgos menos desarrollado, la auditoría basada en riesgos requiere descansar más en la evaluación del riesgo que hace la propia auditoría.

El enfoque de la Auditoría Basada en Riesgos (ABR), tiene como objetivo realizar auditorías priorizando las actividades evaluadas; auditar y generar recomendaciones de mejora sobre los procesos más **críticos** que son identificados luego de un análisis que considera objetivos, riesgos y controles; evaluación que es base para elaborar y actualizar el plan de actividades de auditoría.

Va enfocado al mejoramiento continuo, a la Gestión y el Control claves fundamentales que mejoran y benefician a la cultura del control interno tanto del área de Auditoría Interna como de la Institución Financiera.

El enfoque de auditoría basada en riesgos contempla las siguientes fases:

1. Comprensión de Objetivos y Procesos de negocio relacionados
2. Identificación de Objetivos y Riesgos
3. Evaluación de riesgos
4. Análisis de proceso y riesgo
5. Enfoque de factor riesgo (priorización)
6. Definición del plan

Figura 29, Enfoque de la Auditoría Basada en Riesgos
Fuente: (Badillo, 2010)

3.1. Metodología de valoración de procesos en función de factores de Riesgo

A fin de aplicar una adecuada metodología dentro del área de Auditoría Interna de una Institución Financiera implementando una cultura organizacional que se encuentre basada en la identificación, evaluación y respuestas de los riesgos se validó que se debe crear una metodología de Auditoría Basada en Riesgos la cual como resultados nos arrojaría realizar auditorías de alto impacto, priorizando las actividades de aseguramiento con el fin de auditar y generar recomendaciones de mejora sobre los procesos más críticos que son identificados luego de un análisis que considera objetivos, estrategias, factores de riesgos inherente y de control como base para elaborar y actualizar el plan plurianual de las actividades de auditoría.

En base a la investigación realizada se ha planteado desarrollar la siguiente metodología en el área de Auditoría Interna de la Institución Financiera analizada y pueda ser aplicada por el Director Ejecutivo de Auditoría.

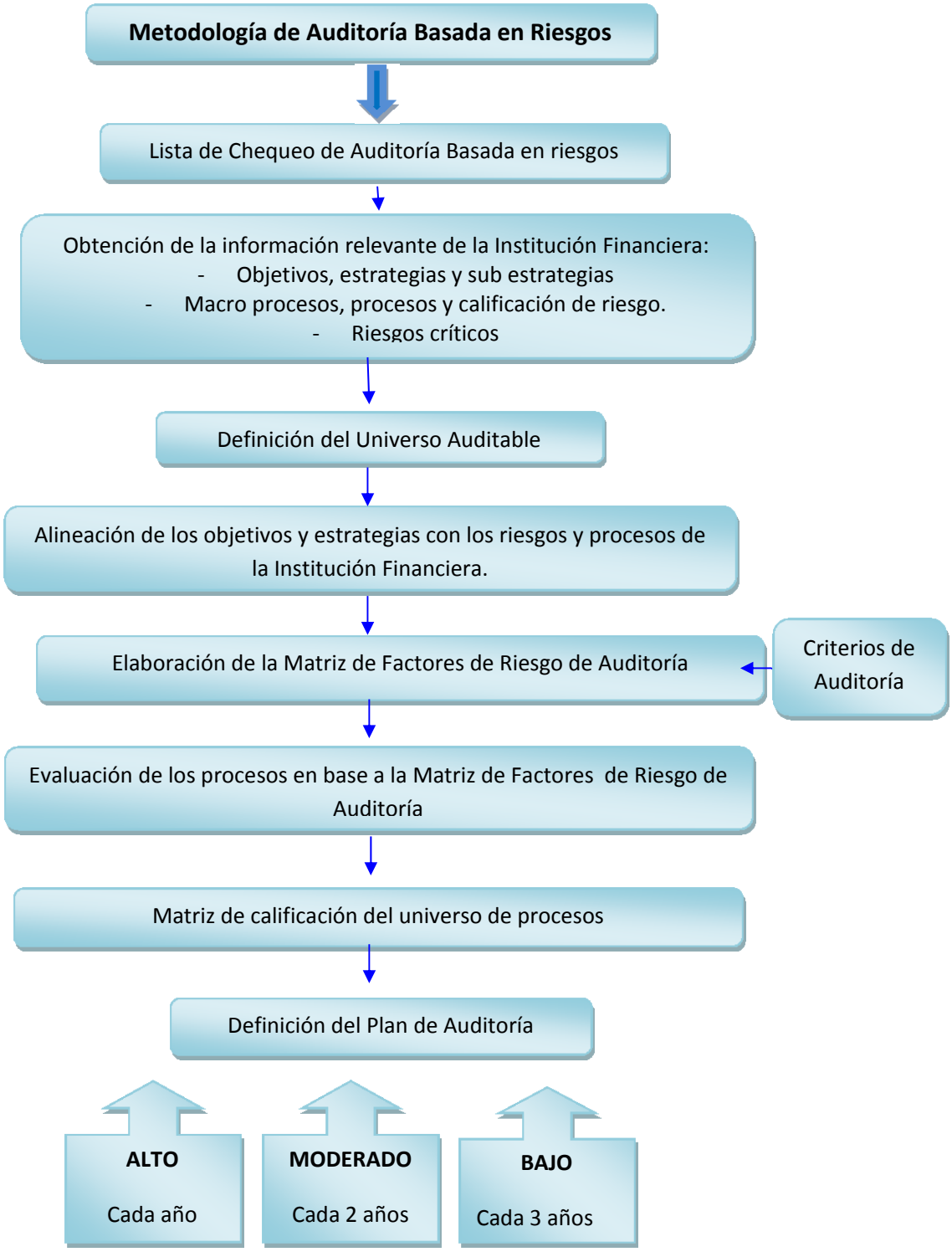


Figura 30, Metodología ABR (Auditoría Basada en Riesgos) según COSO ERM

3.2. Descripción de la Metodología

3.2.1. Lista de chequeo – ABR

Esta lista de chequeo sirve para evaluar los aspectos clave de la planificación y ejecución de auditoría basada en riesgos, a través de la cual se puede identificar áreas de oportunidad para optimizar la aplicación del enfoque de ABR, y que el Auditor tenga un conocimiento general de cómo se está realizando la actividad de la Auditoría Interna y su relación a este enfoque.

Por cuanto se ha considerado tomar como referencia el Ckeck list que emite el Instituto de Auditores Internos donde consta lo siguiente:

- A qué empresa pertenece la evaluación.
- El aspecto clave que se va a evaluar.
- El cumplimiento en el cual se evalúa con un “Si”, “Parcial”, “No”.
- Y la acción requerida que aplica en el caso de un No cumplimiento.

Se emite un puntaje de 1 a cada factor evaluado, y dependiendo de su resultado se evaluará el nivel del enfoque de Auditoría basada en Riesgos en el que se encuentra el área de Auditoría Interna de la Institución Financiera: como resultado podemos obtener las siguientes calificaciones de acuerdo al puntaje total:

- Inexistente 0 % - 10 % de "SI"
- Inicial 11 % - 40 % de "SI"
- Intermedio 41 % - 75 % de "SI"
- Avanzado 76 % - 94 % de "SI"
- Óptimo 95 % - 100 % de "SI"

A continuación se muestra la lista de chequeo:

AUDITORÍA BASADA EN RIESGOS

Lista de chequeo para
Evaluar los aspectos clave de planificación y ejecución de auditoría basada en riesgos - ABR

Unidad de Auditoría Interna de: …….. **Elaborado por:** ……

Fecha: …….. **Aprobado por:** ……..

		Cumplimiento			
No.	**Aspecto Clave**	**Si**	**Parcial**	**No**	**Acción requerida (*)**
	Planificación de las actividades de auditoría con enfoque ABR				
1	¿Está señalado expresamente en el estatuto de auditoría interna que el enfoque del trabajo será de Auditoría Basada en Riesgos - ABR?				
2	¿Está documentada (por escrito y aprobada) la metodología de planificación de las actividades de auditoría interna, incluyendo pasos, criterios, matrices y resultados?				
3	¿El plan de las actividades de auditoría está documentado (por escrito y aprobado)? ¿Es accesible al personal líder de auditoría interna?				
4	¿Para la planificación de las actividades de auditoría interna se considera formalmente mapas de riesgos inherentes y residuales de los procesos clave de la organización (elaborados por la organización o por la misma auditoría interna como insumo interno para planificación)?				
5	¿Para la planificación de las actividades de auditoría interna se considera formalmente: la planeación estratégica y táctica (anual) de la organización, los objetivos y los procesos clave (aquellos que habilitan el logro de los objetivos organizacionales)? ¿Se realiza formal y documentadamente una comprensión del negocio con enfoque top - down?				
6	¿Para la planificación de las actividades de auditoría interna se considera formalmente: los objetivos, riesgos y controles de la organización?				
7	¿Para la planificación de las actividades de auditoría interna se considera formalmente factores de riesgo como: activos en riesgo, visibilidad, complejidad, tamaño del proceso, requerimientos regulatorios externos, estabilidad del control interno, eficacia del control interno, cambios importantes en el proceso y el entorno interno o externo, estado o preocupación de la dirección, resultados de auditorías, etc?				
8	¿Está documentado y se actualiza al menos anualmente el Universo de auditoría?				
9	¿Están definidos y documentados (por escrito y aprobados) ciclos de auditoría?				
10	¿La planificación de auditoría interna es plurianual (de 3 a 5 años) con actualizaciones anuales?				
11	¿El personal de auditoría interna ha recibido entrenamiento (básico y avanzado) sobre gestión de riesgos corporativos?				
12	¿El personal de auditoría interna ha recibido entrenamiento (básico y avanzado) sobre planificación y ejecución de auditoría basada en riesgos?				
13	¿El personal de auditoría interna conoce de manera actualizada el Marco para la Práctica Profesional (definición, normas, código de ética, declaraciones de posición, consejos para la práctica, guías para la práctica) del Instituto de Auditores Internos y como parte de este los lineamientos específicamente relacionados con ABR?				
14	¿En la biblioteca física o electrónica de auditoría interna existe información accesible a todos sobre: Marco para la Practica Profesional del Instituto de Auditores Internos y Gestión de Riesgos Corporativos (COSO ERM, ISO 31.000, IT Risk, etc.)? ¿El equipo de auditoría interna es socio del IAI y puede acceder a la información para socios del web site?				
15	¿Existen plantillas (template) en archivo magnético de los documentos utilizados para la planificación de las actividades de auditoría interna?				

	Ejecución de las actividades de auditoría con enfoque ABR				
16	¿Las actividades de auditoría interna son planificadas con enfoque de auditoría basada en riesgos?				
17	¿En la etapa de planificación de cada actividad específica de auditoría interna se hace una evaluación de los objetivos del proceso a ser auditado?				
18	¿En la etapa de planificación de cada actividad específica de auditoría interna se hace y documenta una identificación de los riesgos que podrían afectar el logro de los objetivos del proceso a ser auditado (incluyendo siempre una evaluación de riegos de fraude del proceso)?				
19	¿En la etapa de planificación de cada actividad específica de auditoría interna se hace y documenta una identificación y posterior evaluación de los controles existentes para afrontar los riesgos del proceso a ser auditado?				
20	¿En la etapa de planificación de cada actividad específica de auditoría interna se hace y documenta un flujograma integral para visualizar: gestión, riesgo y control del proceso a ser auditado?				
	Ejecución de las actividades de auditoría con enfoque ABR				
21	¿En la etapa de planificación de cada actividad específica de auditoría interna se elabora mapas de riesgo inherente y residual reflejando los resultados de la evaluación de control interno?				
22	¿En la etapa de ejecución de trabajo de cada actividad específica de auditoría interna se evalúa el diseño, implementación y funcionamiento de los controles clave existentes para afrontar los riesgos más relevantes del proceso sujeto a auditoría?				
23	¿En la etapa de ejecución de trabajo de cada actividad específica de auditoría interna se desarrolla los hallazgos identificados considerando: condición (lo que sucede), criterio (lo que debería suceder), causa (la causa raíz del hallazgo), y efecto cuantificado (real <problema> y/o potencial <riesgo>)?				
24	¿En la etapa de comunicación de resultados de cada actividad específica de auditoría interna se utiliza una escala (ranking) para categorizar los hallazgos en función del efecto real (problema) y/o potencial (riesgo) del mismo?				
25	¿En las etapas de comunicación y seguimiento de resultados de cada actividad específica de auditoría interna se utiliza escalas cualitatitivas, cuantitativas y colorimétricas para presentar los resultados de la auditoría y el seguimiento a las recomendaciones?				
	Total	0	0	0	

Figura 31, Lista de Chequeo ABR

Fuente: (Badillo, 2010)

A continuación se puede observar el resultado de la aplicación de este check list al área de Auditoría Interna de la Institución Financiera evaluada:

Tabla 4:

Lista de chequeo para Evaluar los aspectos clave de planificación y ejecución de auditoría basada en riesgos

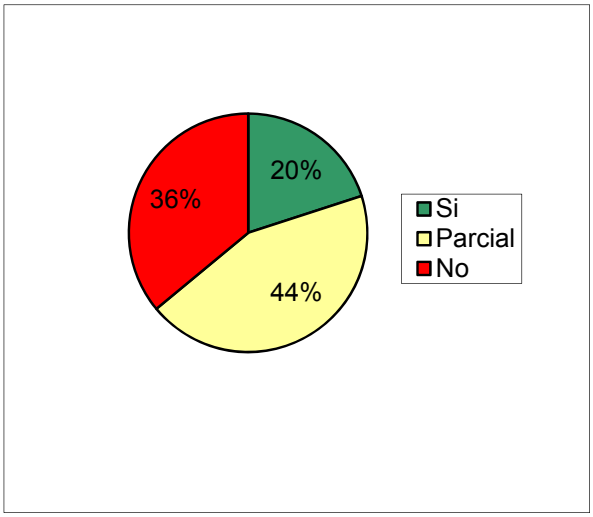
AUDITORÍA BASADA EN RIESGOS	
Lista de chequeo para Evaluar los aspectos clave de planificación y ejecución de auditoría basada en riesgos - ABR	
Unidad de Auditoría Interna de: Institución Financiera	**Elaborado por:** Auditor A
	Revisado por: Auditor Interno - subalterno
Fecha: Quito, 1 de septiembre del 2014	**Aprobado por:** Auditor Interno - Líder

		Cumplimiento			
No.	**Aspecto Clave**	**Si**	**Parcial**	**No**	**Acción requerida (*)**
	Planificación de las actividades de auditoría con enfoque ABR				
1	¿Está señalado expresamente en el estatuto de auditoría interna que el enfoque del trabajo será de Auditoría Basada en Riesgos - ABR?		1		
2	¿Está documentada (por escrito y aprobada) la metodología de planificación de las actividades de auditoría interna, incluyendo pasos, criterios, matrices y resultados?			1	
3	¿El plan de las actividades de auditoría está documentado (por escrito y aprobado)? ¿Es accesible al personal líder de auditoría interna?	1			
4	¿Para la planificación de las actividades de auditoría interna se considera formalmente mapas de riesgos inherentes y residuales de los procesos clave de la organización (elaborados por la organización o por la misma auditoría interna como insumo interno para planificación)?		1		
5	¿Para la planificación de las actividades de auditoría interna se considera formalmente: la planeación estratégica y táctica (anual) de la organización, los objetivos y los procesos clave (aquellos que habilitan el logro de los objetivos organizacionales)? ¿Se realiza formal y documentadamente una comprensión del negocio con enfoque top - down?		1		

		Cumplimiento			
No.	**Aspecto Clave**	**Si**	**Parcial**	**No**	**Acción requerida (*)**
6	¿Para la planificación de las actividades de auditoría interna se considera formalmente: los objetivos, riesgos y controles de la organización?		1		
7	¿Para la planificación de las actividades de auditoría interna se considera formalmente factores de riesgo como: activos en riesgo, visibilidad, complejidad, tamaño del proceso, requerimientos regulatorios externos, estabilidad del control interno, eficacia del control interno, cambios importantes en el proceso y el entorno interno o externo, estado o preocupación de la dirección, resultados de auditorías, etc?	1			
8	¿Está documentado y se actualiza al menos anualmente el Universo de auditoría?	1			
9	¿Están definidos y documentados (por escrito y aprobados) ciclos de auditoría?			1	
10	¿La planificación de auditoría interna es plurianual (de 3 a 5 años) con actualizaciones anuales?		1		
11	¿El personal de auditoría interna ha recibido entrenamiento (básico y avanzado) sobre gestión de riesgos corporativos?		1		
12	¿El personal de auditoría interna ha recibido entrenamiento (básico y avanzado) sobre planificación y ejecución de auditoría basada en riesgos?		1		
13	¿El personal de auditoría interna conoce de manera actualizada el Marco para la Práctica Profesional (definición, normas, código de ética, declaraciones de posición, consejos para la práctica, guías para la práctica) del Instituto de Auditores Internos y como parte de este los lineamientos específicamente relacionados con ABR?	1			
14	¿En la biblioteca física o electrónica de auditoría interna existe información accesible a todos sobre: Marco para la Practica Profesional del Instituto de Auditores Internos y Gestión de Riesgos Corporativos (COSO ERM, ISO 31.000, IT Risk, etc.)? ¿El equipo de auditoría interna es socio del IAI y puede acceder a la información para socios del web site?		1		
15	¿Existen plantillas (template) en archivo magnético de los documentos utilizados para la planificación de las actividades de auditoría interna?			1	
	Ejecución de las actividades de auditoría con enfoque				

		Cumplimiento			
No.	**Aspecto Clave**	**Si**	**Parcial**	**No**	**Acción requerida (*)**
	ABR				
16	¿Las actividades de auditoría interna son planificadas con enfoque de auditoría basada en riesgos?			1	
17	¿En la etapa de planificación de cada actividad específica de auditoría interna se hace una evaluación de los objetivos del proceso a ser auditado?	1			
18	¿En la etapa de planificación de cada actividad específica de auditoría interna se hace y documenta una identificación de los riesgos que podrían afectar el logro de los objetivos del proceso a ser auditado (incluyendo siempre una evaluación de riegos de fraude del proceso)?			1	
19	¿En la etapa de planificación de cada actividad específica de auditoría interna se hace y documenta una identificación y posterior evaluación de los controles existentes para afrontar los riesgos del proceso a ser auditado?		1		
20	¿En la etapa de planificación de cada actividad específica de auditoría interna se hace y documenta un flujograma integral para visualizar: gestión, riesgo y control del proceso a ser auditado?			1	
21	¿En la etapa de planificación de cada actividad específica de auditoría interna se elabora mapas de riesgo inherente y residual reflejando los resultados de la evaluación de control interno?			1	
22	¿En la etapa de ejecución de trabajo de cada actividad específica de auditoría interna se evalúa el diseño, implementación y funcionamiento de los controles clave existentes para afrontar los riesgos más relevantes del proceso sujeto a auditoría?			1	
23	¿En la etapa de ejecución de trabajo de cada actividad específica de auditoría interna se desarrolla los hallazgos identificados considerando: condición (lo que sucede), criterio (lo que debería suceder), causa (la causa raíz del hallazgo), y efecto cuantificado (real <problema> y/o potencial <riesgo>)?		1		
24	¿En la etapa de comunicación de resultados de cada actividad específica de auditoría interna se utiliza una escala (ranking) para categorizar los hallazgos en función del efecto real (problema) y/o potencial (riesgo) del		1		

No.	Aspecto Clave	Cumplimiento			Acción requerida (*)
		Si	Parcial	No	
	mismo?				
25	¿En las etapas de comunicación y seguimiento de resultados de cada actividad específica de auditoría interna se utiliza escalas cualitatitivas, cuantitativas y colorimétricas para presentar los resultados de la auditoría y el seguimiento a las recomendaciones?			1	
	Total	5	11	9	



Conclusión

La Unidad de Auditoría Interna aplica un enfoque de auditoría basado en riesgos en un nivel:

	Inexistente	0 % - 10 % de "SI"
X	**Inicial**	11 % - 40 % de "SI"
	Intermedio	41 % - 75 % de "SI"
	Avanzado	76 % - 94 % de "SI"
	Óptimo	95 % - 100 % de "SI"

Resultado: Posterior a la aplicación utilizando la "Lista de chequeo para Evaluar los aspectos clave de planificación y ejecución de auditoría basada en riesgos – ABR", el área de Auditoría Interna de la Institución Financiera se encuentra en una fase inicial que es del 20%, por cuanto es necesario diseñar una metodología para aplicar la Auditoría Basada en Riesgos y asi determinar una adeucada planificación y cumplir las exigencias de los entes reguladores y brindar un mejor apoyo a la Administracion para el logro de los objetivos institucionales.

3.2.2. Obtención de la información relevante de la Institución Financiera:

Una de las actividades que el Auditor debe realizar es la obtención de la siguiente información relevante que genera la entidad para lograr un entendimiento del negocio:

Objetivos Institucionales: con la finalidad de conocer hacia dónde va enfocada la Institución Financiera y de esta forma apoyar a su cumplimiento en el desarrollo del trabajo de Auditoría.

Estrategias y sub estrategias: Se debe obtener las estrategias y en caso de existir las sub estrategias planteadas por la Entidad Financiera para el logro de los objetivos propuestos. En la presente investigación se consideró el plan estratégico aprobado para el periodo 2012 - 2014.

Macro procesos, procesos: Se debe identificar todos los macro procesos de la entidad para determinar a futuro el Universo de Auditoría. En la Institución Financiera el área que realiza el levantamiento de los procesos es el área de Riesgos. Adicionalmente a estos procesos se debe incorporar al plan las auditorías de cumplimiento regulatorio y proyectos especiales.

Riesgos críticos: Es necesario conocer los riesgos (obstáculos) a los cuales está expuesta la Institución Financiera y podrían impedir el logro de los objetivos institucionales. Esta información se recopila del área de Riesgos quienes son los encargados de realizar el levantamiento y estandarizar la calificación de los procesos de acuerdo a su exposición al riesgo. Se muestra los riesgos identificados para la Institución Financiera:

Tabla 5:

Riesgos críticos

Tipo de Riesgo	Subtipo de Riesgo
Daños a activos materiales	Desastres y otros acontecimientos
Ejecución, entrega y gestión de procesos	Admisión de clientes y documentación
	Contrapartes comerciales
	Distribuidores y proveedores
	Gestión de cuentas de clientes
	Recepción, ejecución y mantenimiento de operaciones
	Seguimiento y comunicación de informes
Fraude Externo	Hurto y fraude
	Seguridad de los sistemas
Fraude Interno	Actividades no autorizadas
	Hurto y fraude
Incidencias en el negocio y fallos en los sistemas	Sistemas
Prácticas con clientes, productos y negocios	Actividades de asesoramiento
	Adecuación, divulgación de información y confianza
	Defectos del producto
	Prácticas inadecuadas de negocio o de mercado
Relaciones laborales y seguridad en el puesto de trabajo	Relaciones laborales
	Salud y seguridad en el puesto de trabajo
Riesgo Legal	Riesgo legal en actividades complementarias de las operaciones del giro financiero
	Riesgo legal en cumplimiento legal y normativo
	Riesgo legal en gestión de crédito
	Riesgo legal en operaciones del giro financiero

Fuente: (Financiera & Riesgos, 2014)

Una vez que se tiene identificados los objetivos de negocio y los procesos clave correspondientes se procede a la identificación de los riesgos que podrían impedir el logro de los objetivos.

La capacidad de comprensión de los riesgos de negocio de parte del auditor interno es fundamental y determinará el grado en que se podrá agregar valor a la organización a través de los trabajos de auditoría interna.

Una vez obtenido esta información se debe elaborar las siguientes matrices:

a) Matriz de Alineación de Objetivos y Estrategias de la Institución financiera versus Riesgos Críticos:

Tabla 6:

Matriz de Objetivos y estrategia vs Riesgos (Institución Financiera)

OBJETIVO	ESTRATEGIAS	SUBESTRATEGIAS	RIESGOS CRÍTICOS (RC)			
			RC1	RC2	RC3	RC4
1	1.1	1.1.1	X		X	
		1.1.2		X	X	X
		1.1.3		X	X	X
	1.2	1.2.1	X			X
		1.2.2	X			X
	1.3	1.3.1		X	X	
2	2.1	2.1.1	X		X	
		2.1.2		X	X	X
		2.1.3		X	X	X
	2.2	2.2.1	X			X
		2.2.2	X			X
	2.3	2.3.1		X	X	

b) Matriz de Alineación de Procesos versus Riesgos Críticos:

Tabla 7:

Matriz de Procesos vs Riesgos (Institución Financiera)

MACROPROCESO	PROCESOS	RIESGOS CRÍTICOS (RC)			
		RC1	RC2	RC3	RC4
1	1.1	X		X	
			X	X	X
			X	X	X
	1.2	X			X
		X			X
	1.3		X	X	
2	2.1	X		X	
			X	X	X
			X	X	X
	2.2	X			X
		X			X
	2.3		X	X	

3.2.3. Definición del Universo Auditable

Tal como se menciona en el Consejo para la Práctica 2010-1, del Instituto de Auditores Internos, el universo de auditoría es un inventario de las auditorías que pudieran realizarse. El DEA puede obtener para este fin, información de parte de la alta dirección, del comité de auditoría; incluir componentes del plan estratégico; objetivos del plan general de negocios y estar normalmente influenciado por los resultados del proceso de gestión de riesgos. Por lo tanto, el calendario de trabajo de auditoría está basado, entre otros factores, de una evaluación de riesgos y exposiciones.

Como se mencionó anteriormente el área que realiza el inventario de los procesos es el área de Riesgos, a quienes fueron solicitados y son los siguientes:

Tabla 8:

Universo de Auditoría (Institución Financiera)

No.	RIESGO OPERATIVO		UNIVERSO DE AUDITORIA
	MACROPROCESO	**PROCESOS**	
1	**GESTIÓN DE COMPRAS, PAGOS Y DISTRIBUCION**	LOGÍSTICA Y DISTRIBUCIÓN DEL EFECTIVO	Transporte de Valores
2	**ADMINISTRACIÓN DE SERVICIOS INSTITUCIONALES**	ADMINISTRACIÓN DE DELIVERY	Delivery
3	**PREVENCIÓN Y CONTROL DE LAVADO DE ACTIVOS**	MONITOREO DE TRANSACCIONES	Formularios G323 (para transacciones superiores a USD 5.000)
			Cumplimiento política Conozca a su Cliente - Formulario G-324
4	**ADMINISTRACIÓN FINANCIERA**	EMISIÓN DE REPORTES	Unidad de Reportes (Proceso emisión)
5	**MANTENIMIENTO**	CANJE Y COMPENSACIÓN	Cámara de compensación (Matriz)
			Cámara de compensación (Sucursales)
6	**SERVICIO AL CLIENTE**	ATENCIÓN EN BALCONES	Arqueo y Revisión de tarjetas Xperta
			Arqueo y Revisión de tarjetas Visa
			Transferencias entre cuentas de clientes
			Chequeras arqueo y entrega
			Cheques devueltos, arqueo y entrega
			Tarjetas E-key, arqueo y entrega
7	**ORIGINACIÓN DE PASIVOS**	APERTURA	Apertura de cuentas de ahorro, corriente
			Inversiones: emisión y pre cancelación
8	**ADMINISTRACIÓN DE SERVICIOS FINANCIEROS (Cash Management)**	AFILIACIÓN DE EMPRESAS	Cash Management, Afiliación de empresas
		LIQUIDACIÓN Y	Cash Management, Liquidación y

No.	RIESGO OPERATIVO		UNIVERSO DE AUDITORIA
	MACROPROCESO	PROCESOS	
		CONTABILIZACIÒN	registro
		CUADRE Y CONCILIACIÒN	Cash Management, Cuadre y conciliación
9	CANALES	CORRESPONSALES NO BANCARIOS	** Corresponsales No Bancarios
10			
11			

** Este proceso no ha sido considerado en el plan de los últimos 3 años

3.2.4. Alineación de los objetivos y estrategias con los riesgos y procesos de la Institución Financiera

La planificación de auditoría basada en riesgos requiere una comprensión general y actualizada del modelo de negocio de la Institución Financiera, esto implica identificar la cadena de valor, los procesos de la organización mapas de proceso y cómo estos se relacionan entre sí para el logro de objetivos. Una vez identificado el Universo Auditable (procesos a auditarse) y conociendo los objetivos y estrategias de la entidad, y para identificar a que objetivos y estrategias apoyan los diferentes procesos auditados se debe elaborar una matriz en la cual se observe claramente este alineamiento.

Para ejemplificar se ha seleccionado los procesos del área de Auditoría de operaciones los cuales se muestran en la siguiente matriz:

Tabla 9:

Matriz de objetivos y estrategias con los riesgos (Institución Financiera)

OBJETIVO	ESTRATEGIAS	SUBESTRATEGIAS	RIESGOS POTENCIALES (RIESGO OPERATIVO)																						
			Daños a activos materiales	Ejecución, entrega y gestión de procesos						Fraude Externo		Fraude Interno		Incidencias / negocio y fallos / sistemas	Prácticas con clientes, productos y negocios				Relaciones laborales y seg. en el puesto de trabajo		Riesgo Legal			
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
GENERACIÓN DE VALOR ECONÓMICO INCREMENTAL PARA	1) Identificación, entendimiento, fidelización y maximización de valor de los clientes del mercado objetivo, durante su ciclo de vida.	Potencialización del Modelo de conocimiento y entendimiento del cliente y mercado.		X				X	X									X				X		
		Retención de clientes (disminución de deserción).		X				X	X									X				X		
		Ampliación estratégica en cobertura de los canales y Direccionamiento en el uso de Canales Alternativos.		X				X	X									X				X		
		Potencialización y crecimiento en la relación con los clientes y adquisición de nuevos.		X				X	X									X				X		
	2) Generación de ventaja competitiva en calidad, productividad e innovación, entregando productos y	Mejora continua del Modelo de Negocio y Riesgo apalancados en un Modelo Tecnológicos y operativo dinámico y eficiente.	X	X	X	X	X	X		X	X	X	X	X		X		X			X	X	X	X
		Consolidar el Modelo de Productividad y Calidad de Servicio (Implementación de Mejores prácticas y acuerdos de servicio).	X	X	X	X	X	X		X	X	X	X	X		X		X			X	X	X	X

OBJETIVO	ESTRATEGIAS	SUBESTRATEGIAS	RIESGOS POTENCIALES (RIESGO OPERATIVO)																					
			Daños a activos materiales	**Ejecución, entrega y gestión de procesos**						**Fraude Externo**		**Fraude Interno**		**Incidencias / negocio y fallos / sistemas**	**Prácticas con clientes, productos y negocios**				**Relaciones laborales y seg. en el puesto de trabajo**		**Riesgo Legal**			
			1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**
	servicios, más rápido y mejor que la competencia	Reconocer al recurso humano como factor estratégico a través de una administración planificada, eficiente, oportuna y de calidad, vinculada a un modelo integral de desempeño.	**X**	**X**	**X**	**X**	**X**	**X**		**X**	**X**	**X**	**X**	**X**		**X**		**X**			**X**	**X**	**X**	**X**
		Crear productos y servicios financieros innovadores, rentables, primeros en el mercado, fáciles de utilizar generando una percepción de valor al cliente.	**X**	**X**	**X**	**X**	**X**	**X**		**X**	**X**	**X**	**X**	**X**		**X**		**X**			**X**	**X**	**X**	**X**
	3) Obtención de resultados financieros sostenidos y superiores garantizando la solvencia y la adecuada administración de riesgos	Administración del Modelo Gerencial basado en la medición y seguimiento a través de presupuestos financieros, rentabilidad por línea de negocio, proyectos, objetivos inter áreas, e indicadores de gestión, calidad y productividad				**X**	**X**	**X**				**X**	**X**	**X**							**X**	**X**	**X**	**X**
		Administración del Modelo de Riesgo que garantice la Calidad de Activos de Riesgo y minimice la probabilidad de pérdidas.				**X**	**X**	**X**				**X**	**X**	**X**							**X**	**X**	**X**	**X**

OBJETIVO	ESTRATEGIAS	SUBESTRATEGIAS	RIESGOS POTENCIALES (RIESGO OPERATIVO)																						
			Daños a activos materiales	**Ejecución, entrega y gestión de procesos**						**Fraude Externo**		**Fraude Interno**		**Incidencias / negocio y fallos / sistemas**	**Prácticas con clientes, productos y negocios**				**Relaciones laborales y seg. en el puesto de trabajo**		**Riesgo Legal**			
			1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**
		Gestionar el Modelo de Aprobación Crediticia y Cobranza basándonos en las mejores prácticas.				X	X	X				X	X	X							X	X	X	X
	4) Integrar en las actividades de la Organización principios de responsabilidad social y compromiso con la sociedad, sus colaboradores y el medio ambiente.	Fomentar prácticas de buen gobierno corporativo, etica y transparencia en el Modelo de Gestión.						X	X	X			X					X	X	X		X		
		Promover el desarrollo del talento personal, familiar y profesional de los colaboradores, incorporando las prácticas de RS en la Cultura Organizacional.						X	X	X			X					X	X	X		X		
		Fomentar prácticas de Responsabilidad Social en la relación con los clientes y proveedores.						X	X	X			X					X	X	X		X		
		Realizar programas que incluyan en el Modelo de Gestión la preservación y el cuidado del Medio Ambiente y los Recursos No Renovables.						X	X	X			X					X	X	X		X		

Descripción de los Riesgos Potenciales de la Institución Financiera:

Tipo de Riesgo	No. Subtipo de Riesgo	Subtipo de Riesgo
Daños a activos materiales	**1**	Desastres y otros acontecimientos
Ejecución, entrega y gestión de procesos	**2**	Admisión de clientes y documentación
	3	Contrapartes comerciales
	4	Distribuidores y proveedores
	5	Gestión de cuentas de clientes
	6	Recepción, ejecución y mantenimiento de operaciones
	7	Seguimiento y comunicación de informes
Fraude Externo	**8**	Hurto y fraude
	9	Seguridad de los sistemas
Fraude Interno	**10**	Actividades no autorizadas
	11	Hurto y fraude
Incidencias / negocio y fallos / sistemas	**12**	Sistemas
Prácticas con clientes, productos y negocios	**13**	Actividades de asesoramiento
	14	Adecuación, divulgación de información y confianza
	15	Defectos del producto
	16	Prácticas inadecuadas de negocio o de mercado
Relaciones laborales y seguridad en el puesto de trabajo	**17**	Relaciones laborales
	18	Salud y seguridad en el puesto de trabajo
Riesgo Legal	**19**	Riesgo legal en actividades complementarias de las operaciones del giro financiero
	20	Riesgo legal en cumplimiento legal y normativo
	21	Riesgo legal en gestión de crédito
	22	Riesgo legal en operaciones del giro financiero

Resultado: Al mapear en esta matriz los objetivos versus los riesgos el auditor puede visualizar de manera general que riesgos pueden afectar a la consecución del objetivo institucional y a sus diferentes estrategias, dándole un mayor conocimiento de los riesgos

más críticos que pueden afectar a la Institución Financiera y tener como un marco de referencia para desarrollar su planificación de Auditoría.

Tabla 10:

Matriz de procesos y riesgos (Institución Financiera)

No.	Proceso	RIESGOS POTENCIALES (RIESGO OPERATIVO)																						Tot
		Daños a activos materiales	Ejecución, entrega y gestión de procesos						Fraude Externo		Fraude Interno		Incidencias / negocio y fallos / sistemas	Prácticas con clientes, productos y negocios				Relaciones laborales y seg. en el puesto de trabajo		Riesgo Legal				
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	
1	Transporte de Valores	X	X	X			X	X	X		X	X			X			X	X	X			X	13
2	Corresponsales No Bancarios	X	X		X	X	X		X	X	X	X	X	X	X	X				X	X	X		16
3																								
4																								
5																								
6																								

Descripción de los Riesgos Potenciales de la Institución Financiera:

No. Subtipo de Riesgo	Subtipo de Riesgo
1	Desastres y otros acontecimientos
2	Admisión de clientes y documentación
3	Contrapartes comerciales
4	Distribuidores y proveedores
5	Gestión de cuentas de clientes
6	Recepción, ejecución y mantenimiento de operaciones
7	Seguimiento y comunicación de informes
8	Hurto y fraude
9	Seguridad de los sistemas
10	Actividades no autorizadas
11	Hurto y fraude
12	Sistemas

13	Actividades de asesoramiento
14	Adecuación, divulgación de información y confianza
15	Defectos del producto
16	Prácticas inadecuadas de negocio o de mercado
17	Relaciones laborales
18	Salud y seguridad en el puesto de trabajo
19	Riesgo legal en actividades complementarias de las operaciones del giro financiero
20	Riesgo legal en cumplimiento legal y normativo
21	Riesgo legal en gestión de crédito
22	Riesgo legal en operaciones del giro financiero

Resultado: En el mapeo de esta matriz observamos que la Institución Financiera está expuesta a 22 riesgos potenciales al realizar la evaluación de 2 procesos obtuvimos que el proceso de Transporte de Valores está expuesto a 13 riesgos y el proceso de Corresponsales No Bancarios a 16 riesgos, al realizar la validación con todos los procesos que forman parte del universo de Auditoría versus los potenciales riesgos el auditor podrá visualizar los riesgos a los cuales están expuestos los procesos que se desarrollan en la Institución, dando una alerta de que procesos debe poner mayor atención al momento de realizar su planificación. En el Ejemplo presentado el proceso de Corresponsales No Bancarios está expuesto a más riesgos que el proceso de Trasporte de Valores.

3.2.5. Elaboración de la Matriz de Factores de Riesgo de Auditoría

La Matriz de factores de riesgo es primordial para realizar la Planificación de Auditoría basada en riesgo.

En base a la investigación realizada se muestra y se describe la matriz desarrollada para evaluar los procesos, previo a la planificación:

Tabla 11:

Matriz Detallada de Factores de Riesgo para evaluación de procesos

Factores de Riesgo	**Puntaje del Factor de Riesgo**	**Explicación de Evaluación**
FACTORES DE RIESGO INHERENTE		
A. Complejidad y tamaño de la Operación		
Complejidad de la Operación	**5**	
Subprocesos que intervienen en el proceso	5	1 : hasta 1 subprocesos 2: hasta 2 subprocesos 3: hasta 3 subprocesos 4: hasta 4 subprocesos 5: más de 5 subprocesos
Áreas que participan en el proceso	5	1 : una sola área 2 - 3 : 2 a 3 áreas 4 - 5: más de 3 áreas
Participación de proveedores externos (empresas de servicios)	5	0: sin intervención 1 : Participa en el proceso una empresas 2: Participa en el proceso dos empresas 3: Participan en el proceso más de tres empresas Entre 1 y 2 puntos adicionales por mala experiencia con los proveedores (niveles de servicio)
Complejidad en las actividades / procedimientos en la ejecución del proceso	5	1 : Tareas simples y no especializadas 2 - 3 : La actividad requiere varias tarea especializadas (requiere criterio) y la interacción de varias personas 4 - 5 : Varios tareas especializadas que requieren coordinación de varias personas en el proceso y con otros procesos.
Grado de automatización	**5**	
Número de aplicativos tecnológicos que intervienen en el proceso	**5**	1 : un solo aplicativo 2 : 2 aplicativos 3 - 5 : más de 2 aplicativos que intervienen en el proceso
Número de operaciones	**5**	0 : sin operaciones manuales (100% operaciones automáticas)

Factores de Riesgo	Puntaje del Factor de Riesgo	Explicación de Evaluación
automatizadas y/o manuales		1 : hasta 10% del total de operaciones manuales. 2 - 3: entre el 11% y el 25% de operaciones manuales 4 - 5: más del 25%
Cambios importantes en la tecnología y nivel de obsolescencia	**5**	0 : Sin cambios en los últimos 12 meses 1 : Con cambios en los últimos 12 meses 2 - 3: Algunos cambios en la tecnología (sistemas) con cierto impacto en los últimos 12 meses. 4 : Cambios importante en el negocio o en el proceso o nuevo sistema de tecnología en los últimos 12 meses. 5 : Obsolescencia de aplicativos tecnológicos.
Registro contable de las operaciones	**5**	
Registro contable de las operaciones (frecuencia versus parametrización).	5	1 - 2: operaciones donde en registro contable es rutinario y parametrizado. 3- 4: operaciones donde el registro contable es rutinario y no parametrizado. 5: operaciones donde el registro contable no es rutinario y no parametrizado.
Valor monetario en exposición	5	1 - : hasta el 5% de la materialidad de auditoría (*) 2 - 3: entre 6% y 15% 4 - 5: más del 15%.
B. Naturaleza del Entorno de Negocios		
Complejidad de leyes y regulaciones.	**5**	
Normativa legal y su complejidad en los procesos	5	0 - 1: Normativa legal no compleja 2 - 3: Alguna normativa legal con cierta complejidad 4 - 5: Cantidad importante de normativa legal y muy compleja
Historia de pérdidas por fraude y errores externos	**5**	
Fraudes, robos y asaltos	5	Se obtiene conforme el valor en exposición (pérdida neta) en relación la materialidad establecida para el proceso/cuenta (pérdida neta/materialidad *5)

Factores de Riesgo	Puntaje del Factor de Riesgo	Explicación de Evaluación
Fallas en el servicio de proveedores (Incumplimiento de niveles de servicio) que originaron reclamos de clientes (incluido fraude)	5	0 - 1: Eventuales reclamos de clientes de insignificante valor material en los últimos 12 meses 2 - 3: Eventuales reclamos de clientes de valor material importante en los últimos 12 meses 4 - 5: Continuos reclamos de clientes de valor importante en los últimos 12 meses (considerar la materialidad establecida para el proceso)
C. Naturaleza Interna de la Entidad		
Historia de pérdidas por fraude y errores internos	**5**	
Fraudes informáticos	5	0 - 1: Sin historial importante en número y monto 2 - 3: Varios casos de fraude, debilidad del Control Interno o fallas en el cumplimiento de políticas y procedimientos pero no de gran importancia en los últimos 12 meses. 4 - 5: Debilidades del Control Interno o fallas en el cumplimiento de políticas y procedimientos de gran importancia en los últimos 12 meses, que originaron fraude interno.
Fraudes cometidos por el personal del Banco	5	0 - 1: Sin historial importante en número y monto 2 - 3: Varios casos de fraude, debilidad del Control Interno o fallas en el cumplimiento de políticas y procedimientos pero no de gran importancia en los últimos 12 meses. 4 - 5: Debilidades del Control Interno o fallas en el cumplimiento de políticas y procedimientos de gran importancia en los últimos 12 meses, que originaron fraude interno.
Error u omisión en la ejecución de los procesos	5	0 - 1: Sin historial importante en número y monto 2 - 3: Varios casos de errores u omisiones en la ejecución del proceso pero no de gran importancia en los últimos 12 meses. 4 - 5: Varios casos de errores u omisiones en la ejecución del proceso de gran importancia en los últimos 12 meses, que originaron pérdidas económicas para la entidad financiera.
Rotación de Personal	**5**	

Factores de Riesgo	Puntaje del Factor de Riesgo	Explicación de Evaluación
Rotación de personal clave y niveles de supervisión	5	0: sin rotación en los últimos 12 meses de los funcionarios 1-2: salida del supervisor 3-4: salida del responsable 5 : salida del vicepresidente
Alta rotación del personal operativo	5	Corresponde al porcentaje de rotación del personal del área auditada, (Porcentaje de Rotación*5). Información que debe ser solicitada a la Unidad de RRHH.
Planes de sucesión y backups	5	0 : Existencia de planes de sucesión y backups. 1 - 2: Planes de sucesión y backups incompletos hasta el 50% 3 - 4 : Planes de sucesión y backups incompletos más del 50% 5 : Falta de planes de sucesión y backups
Comisiones del personal	**5**	
Incentivo adicional a la remuneración básica	**5**	0 : no existen comisiones 1 - 2: comisiones sin efecto importante (hasta el 5%) 3 - 4: comisiones entre el 6% y el 20% 5 : las comisiones son mayores del 21% al 30% en relación con la remuneración.
FACTORES DE RIESGO DE CONTROL		
A. Cumplimiento de políticas, procedimientos y normativa legal		
Diseño e implementación de políticas y procedimientos	**5**	
Existencia de manuales (políticas y procedimientos por escrito) y que se encuentran aprobadas	5	0 : Existen manuales aprobador por el Directorio 1 - 2: Existen manuales actualizados sin aprobación del Directorio 3 -4 : Manuales en proceso de elaboración que no están revisados ni aprobados 5 : No existen manuales.
Adecuadas y claros niveles de autorización	**5**	

Factores de Riesgo	**Puntaje del Factor de Riesgo**	**Explicación de Evaluación**
Existencia de manual de funciones	5	0 : Existencia de manuales de funciones actualizados 1 - 2: Las funciones se encuentran desactualizadas en manuales, pero no existe mayor incidencia en los procesos. 3 -4 : Las funciones se encuentran desactualizadas en manuales y existe importante incidencia en los procesos 5 : No existen manuales de funciones
Existencia de adecuados niveles de autorización	5	0 : Existen niveles de autorización aprobados 1 - 3: Existen niveles de autorización no aprobados 4 - 5: No existen niveles de autorización
Cumplimiento de leyes y reglamentos relevantes por parte del personal clave	**5**	
Multas y sanciones por el no cumplimiento de regulaciones de entes de control	5	0 : No existencia de sanciones y multas para el personal clave y/o la entidad financiera. 1 - 2: Multas para el personal clave y/o la entidad financiera. 3 - 4: Posibilidad de destitución de personal clave 5 : Posibilidad de cierre temporal de las operaciones en sucursales y/o la entidad financiera.
Nivel de cumplimiento con políticas y procedimientos relevantes.	**5**	
Nivel de cumplimiento de políticas y procedimientos por parte del personal clave.	5	0 - 1: No existe incumplimiento del personal clave 2 - 3: Incumplimiento de políticas y procedimientos por funcionarios claves que no afectan significativamente el proceso 4 - 5: Incumplimiento de varias políticas y procedimientos por funcionarios claves que afectan significativamente el proceso
B. Estructura y Eficacia del Control Interno		
Reportes para el monitoreo de las operaciones	**5**	

Factores de Riesgo	Puntaje del Factor de Riesgo	Explicación de Evaluación
Existencia de reportes para monitorear las operaciones.	5	0 : Existen definidos reportes, procedimientos formales y funcionarios responsables para el monitoreo. 1 -2: Existen reportes, y monitoreo no frecuente y no se han definido procedimientos ni funcionarios responsables. 3 -4: Existen reportes, no se realizan monitoreo y no se han definido funcionarios responsables. 5 : No existen reportes, procedimientos y tampoco se han definido funcionarios responsables.
Apropiados niveles de supervisión y revisión	**5**	
Adecuada segregación de funciones	5	0 : Existe adecuada segregación de funciones. 1 : Algunas actividades que no afectan significativamente el proceso, no tienen una adecuada segregación de funciones 2-3: Gran parte de las actividades que pueden afectar significativamente al proceso no se encuentran segregadas. 4-5: Ausencia total de segregación de funciones.
Evidencia de revisión y supervisión	5	0 : Existe evidencia de supervisión 1 - 2: Existe supervisión pero no existe una adecuada evidencia. 3 - 4 : No existe supervisión y evidencia en procedimientos significativos. 5 : No existe supervisión
Conocimiento y habilidades del personal	**5**	
Personal del área cumple con el perfil requerido para el cargo	5	0 : Personal cumple con el perfil requerido para los diferentes cargos 1 - 3: Personal cumple parcialmente con el perfil requerido para los cargos. 4 - 5: Personal no cumple con el perfil requerido para los cargos asignados.
Experiencia en el desempeño de funciones	5	0 - 1: Desempeño de funciones en el cargo mayor a tres años y demuestra efectividad y eficiencia. 2 - 3: Desempeño entre 1 y 3 años en las funciones y su efectividad y eficiencia están en proceso de afianzamiento. 4 : Desempeño de las funciones o cargos similares

Factores de Riesgo	Puntaje del Factor de Riesgo	Explicación de Evaluación
		hasta un año. 5 : Sin experiencia en el cargo o funciones similares.
Existencia de planes de capacitación	5	0 : El personal ha recibido capacitación formal (interna o externa) con respecto a las políticas y procedimientos, aspectos legales, relacionados con el cargo, en los últimos 12 meses; o, no han existido cambios relevantes en sus funciones. 1 - 3: El personal ha recibido capacitación formal con respecto a sus funciones, en un tiempo mayor a 12 meses. 5 : No existe capacitación ni un plan anual.
Adecuados controles físicos para evitar el acceso a datos, operaciones y áreas restringidas	**5**	
Controles duales en cajas y bóvedas	5	0 : Se cumplen con los controles duales. 5: No se cumplen con los controles duales.
Cajas fuertes para custodia de efectivo (procesos relacionados en sucursales)	5	0 : Existen y se utilizan cajas fuertes 5: No existen o no se utilizan cajas fuertes
Sistema de archivo de documentos relevantes	5	0 : Archivo adecuado de documentación relevante en cajas de seguridad 1 -2 : Sistema de archivo físico no es caja de seguridad, pero brinda salvaguarda adecuada. 3 - 4: Los documentos relevantes se resguardan en un archivador simple sin acceso restringido. 5 : El sistema de archivo no brinda ningún tipo de seguridad.
Controles de acceso a áreas de la Institución, tanto a funcionarios como a personas externas.	5	0 : Existen sistemas automáticos que capturan el ingreso/salida de personas y son efectivos. 1 - 2: El control de acceso se realiza mediante bitácoras manuales y las mismas son validadas por parte de un funcionario independiente en forma periódica. 3 - 4: Existen sistemas automáticos/manuales; sin embargo, no funcionan y/o no cuentan con monitoreo adecuado. 5 : No existen sistemas automáticos ni manuales para el control de acceso.

Factores de Riesgo	**Puntaje del Factor de Riesgo**	**Explicación de Evaluación**
Sistemas de seguridad (alarmas, monitoreo de entrada y salida)	5	0 : Existen sistemas de seguridad: alarmas, monitoreo de entrada y salida, cámaras y guardianía (de ser necesario). 1 - 2: Existen sistemas de seguridad: alarmas, monitoreo de entrada y salida, no existen cámaras ni vigilancia armada (guardias). 3 - 4: Los sistemas han presentado deficiencias. 5 : No existen sistemas de seguridad.
Seguridades de los sistemas informáticos	5	Considerar: a. Perfiles de acceso están conforme a funciones b. Presencia de usuarios autorizados. c. Existencia de logs de auditoría (rastro de las transacciones) d. Inexistencia de usuarios genéricos ---------- 0 : Cumplimiento de a),b), c), d). 2 : Cumple al menos 3 de los factores 3 : Cumple al menos 2 de los factores. 4 - 5: No cumple ninguno de estos factores.
Grado de implementación de recomendaciones de auditorías anteriores	**5**	
Observaciones no regularizadas de anteriores auditorías	5	0: Todas las observaciones de Auditorías anteriores fueron implementadas 1: hasta el 5% de observaciones 2: entre 6% y 15% 3: más del 15%. Un punto adicional para observaciones de Riesgo Moderado y dos puntos para las de Riesgo Alto
Reincidencia de las observaciones no regularizadas (Se refiere a observaciones que fueron regularizadas pero su incumplimiento se convirtió en recurrente).	5	1: hasta el 5% de observaciones de la presente revisión son reincidentes 2: entre 6% y 15% 3: más del 15%. Un punto adicional para observaciones de Riesgo Moderado y dos puntos para las de Riesgo Alto.
C. *Calidad e Integridad de la Información Financiera e Información Gerencial.*		

Factores de Riesgo	Puntaje del Factor de Riesgo	Explicación de Evaluación
Adecuados sistemas de información gerencial	**5**	
Los sistemas que intervienen en el proceso, emiten reportes gerenciales	5	0 : El sistema emite reportes gerenciales y son utilizados por el personal clave. 1 - 3: El sistema emite reportes gerenciales y no son utilizados por el personal clave 4 - 5: El sistema no emite reportes gerenciales
Emisión de reportes (automáticos y manuales)	5	0 : Todos los reportes son automáticos 1 -2: Los reportes manuales corresponden a un 25% de la información relevante. 3 -4 : Los reportes manuales corresponden hasta un 50% de la información relevante. 5 : Más del 50% de los reportes son manuales.
Integridad de las fuentes de información	**5**	
Integridad de las bases de datos	5	0: Las bases de datos que intervienen en el proceso, provienen de sistemas cerrados, en los cuales no es posible la manipulación. 5: Las bases de datos que intervienen en el proceso, no provienen de sistemas cerrados y/o es posible la manipulación.
Revisión independiente y conciliación de la información	**5**	
Frecuencia de la conciliación de la información	5	0 : Se realiza una conciliación frecuente y oportuna (diaria, semanal, mensual, etc., dependiendo de la naturaleza de cada proceso) 1 - 2: Los reportes se concilian pero presentan diferencias inmateriales. 3 - 4: Se realiza una conciliación de manera esporádica y las diferencias son importantes y no regularizadas 5 : No se realizan conciliaciones de la información.
D. Efectividad de la Gerencia		
Efectividad de la gerencia (monitoreo y control)	**5**	

Factores de Riesgo	Puntaje del Factor de Riesgo	Explicación de Evaluación
La gerencia investiga y monitorea continuamente (fuentes internas y externas) sobre los riesgos que afectan a la organización y a su proceso	5	0 : Existe un sistema/procedimiento formal debidamente aprobado para la investigación y monitoreo de riesgos, el cual se aplica sistemáticamente. 1 -2: Existe un sistema/procedimiento formal para la investigación y monitoreo de riesgos, sin embargo su aplicación ha alcanzado máximo un 75% del total del proceso/cuenta. 3 -4 : Existe un sistema/procedimiento formal para la investigación y monitoreo de riesgos, sin embargo es obsoleto o insuficiente para su propósito final. 5 : No existe un sistema de investigación ni monitoreo de riesgos.
La gerencia actualiza los manuales de procedimientos conforme los nuevos requerimientos del proceso (riesgo y controles), en forma oportuna.	5	0 : La actualización de manuales es inmediata, conforme a los cambios del proceso (máximo 30 días). 1 -2: La actualización de manuales es mediata, conforme a los cambios del proceso (máximo 60 días). 3 -4 : La actualización de manuales es tardía, frecuencia mayor a 60 días. 5 : No existe actualización de manuales, conforme los cambios del proceso.
Conocimiento, experiencia y habilidad	**5**	
Perfil profesional conforme funciones	5	0 : El perfil profesional de la gerencia corresponde con las funciones asignadas 1 - 3: El perfil profesional corresponde parcialmente con los requerimientos del cargo. 4 - 5: El perfil no está de acuerdo con las funciones que desempeña y son totalmente diferentes al perfil del puesto.
Experiencia profesional	5	0 - 1: Experiencia mayor a tres años y demuestra efectividad y eficiencia en el cargo. 2 - 3: Experiencia entre 1 y 3 años en las funciones y su efectividad y eficiencia están en proceso de afianzamiento. 4 : Experiencia profesional hasta un año en las funciones que desempeña o en cargos similares. 5 : Sin experiencia en el cargo o funciones similares.
Adecuada supervisión	**5**	

Factores de Riesgo	Puntaje del Factor de Riesgo	Explicación de Evaluación
Frecuencia y oportunidad de la supervisión	5	0 : Evidencia de supervisión continua y oportuna y seguimiento a instrucciones. 1 - 2: Evidencia de supervisión; sin embargo, las principales decisiones tomadas, no se han implantado en forma oportuna y adecuada. 3 - 4: Supervisión no regular. 5 : No existe supervisión.
Adecuada comunicación de la gerencia	**5**	
Comunicación de la información oportuna	5	0 : La transmisión de información relevante es oportuna y por escrito. 1 - 3: La información se comunica en forma verbal y se efectúan comunicaciones por escrito con cierta demora (hasta una semana). 4 - 5: No existe evidencia de transmisión de información y decisiones relevantes.
Uso de reportes gerenciales para medir y monitorear	**5**	
Utilización de reportes que faciliten el monitoreo de las operaciones y el cumplimiento de los controles implantados.	5	0 : Utilizan reportes únicamente automatizados para el monitoreo y supervisión de las operaciones; adicionalmente, éstos arrojan alertas a través de la cuales se pueden implementar mejores controles. 1 - 2: Utilizan reportes manuales y automatizados para el monitoreo y supervisión de las operaciones. 3 - 4: No se han incluido en el sistema de reportes todos los informes necesarios para toma de decisiones. 5 : No utilizan reportes para el monitoreo de las operaciones.
Utilización de presupuestos para evaluación		0 : Se realizan evaluaciones mensuales del presupuesto. 1 - 2: Las evaluaciones presupuestarias se efectúan por períodos mayores a un mes (hasta 3 meses). 3 - 4: El análisis presupuestario se realiza en forma esporádica (mayor a 3 meses). 5 : El área no realiza evaluaciones periódicas del presupuesto o no existe presupuesto.

Factores de Riesgo	Puntaje del Factor de Riesgo	Explicación de Evaluación
Existencia de comités o juntas. Se emiten actas donde se resumen las principales decisiones.	5	0 : Existen actas de los comités donde se incluyen las decisiones tomadas y éstas se encuentren debidamente foliadas, enumeradas y con las firmas respectivas y archivadas adecuadamente. 1 - 3: Las actas se oficializan vía e-mail entre los asistentes a los comités, sin embargo, no se mantiene un control del archivo (electrónico o físico) de dichas comunicaciones. 4 - 5: Los comités no formalizan las decisiones mediante actas o algún documento similar.

Tabla 12:

Matriz Resumen de Factores de Riesgo para evaluación de procesos

Factores de Riesgo	Puntaje del Factor de Riesgo	Ponderación de Riesgo	Riesgo ponderado calculado
FACTORES DE RIESGO INHERENTE			
A. Complejidad y tamaño de la Operación			
Complejidad de la Operación	5	40%	2
Grado de automatización	5	30%	1,5
Registro contable de las operaciones	5	30%	1,5
Subtotal		100%	5
B. Naturaleza del Entorno de Negocios			
Complejidad de leyes y regulaciones.	5	60%	3
Historia de pérdidas por fraude y errores externos	5	40%	2
Subtotal		100%	5
C. Naturaleza Interna de la Entidad			
Historia de pérdidas por fraude y errores internos	5	40%	2
Rotación de Personal	5	30%	1,5

Factores de Riesgo	Puntaje del Factor de Riesgo	Ponderación de Riesgo	Riesgo ponderado calculado
Comisiones del personal	5	30%	1,5
Subtotal		100%	5
TOTAL RATIO DE RIESGO INHERENTE		**Alto**	**15**
FACTORES DE RIESGO DE CONTROL			
A. Cumplimiento de políticas, procedimientos y normativa legal			
Diseño e implementación de políticas y procedimientos	5	25%	1,25
Adecuadas y claros niveles de autorización	5	25%	1,25
Cumplimiento de leyes y reglamentos relevantes por parte del personal clave	5	25%	1,25
Nivel de cumplimiento con políticas y procedimientos relevantes.	5	25%	1,25
Subtotal		100%	5
B. Estructura y Eficacia del Control Interno			
Reportes para el monitoreo de las operaciones	5	20%	1
Apropiados niveles de supervisión y revisión	5	20%	1
Conocimiento y habilidades del personal	5	20%	1
Adecuados controles físicos para evitar el acceso a datos, operaciones y áreas restringidas	5	20%	1
Grado de implementación de recomendaciones de auditorías anteriores	5	20%	1
Subtotal		100%	5
C. ***Calidad e Integridad de la Información Financiera e Información Gerencial.***			
Adecuados sistemas de información gerencial	5	30%	1,5
Integridad de las fuentes de información	5	30%	1,5
Revisión independiente y conciliación de la	5	40%	2

Factores de Riesgo	Puntaje del Factor de Riesgo	Ponderación de Riesgo	Riesgo ponderado calculado
información			
Subtotal		100%	5
D. Efectividad de la Gerencia			
Efectividad de la gerencia (monitoreo y control)	5	20%	1
Conocimiento, experiencia y habilidad	5	20%	1
Adecuada supervisión	5	20%	1
Adecuada comunicación de la gerencia	5	20%	1
Uso de reportes gerenciales para medir y monitorear	5	20%	1
Subtotal		100%	5
TOTAL RATIO DE RIESGO DE CONTROL		**Bajo**	**20,00**
TOTAL RATIO DE RIESGO AGREGADO		**Alto**	**35,00**

Descripción de los elementos que forman parte de la matriz

Factores de riesgo: La vinculación de procesos de negocio y riesgos se realiza a través de los factores de riesgo utilizados para evaluar los riesgos en los procesos (enfoque de factores de riesgo). En todas las empresas existen riesgos, pero algunos imposibles de eliminar; sin embargo, el panorama de factores de riesgo permite identificarlos y visualizar de forma general como se encuentra el proceso y en algunos casos estos factores ayudan a determinar ciertas debilidades de control interno y las acciones que se pueden implementar para mitigarlos.

Con el objeto de limitar la existencia de subjetividad en la evaluación, soportar y facilitar el análisis de los factores de riesgo, estos fueron ampliados en sub factores, en los cuales, cada uno de ellos incluye criterios de evaluación.

Los factores de riesgo están relacionados generalmente con el alcance de las actividades de control diseñadas en los procesos con el propósito de asegurar que se logre sus objetivos, con el apoyo del personal que participa en el desarrollo de las actividades y la gestión del proceso y el entorno y naturaleza en el que este funciona.

Explicación de evaluación y puntaje del factor de riesgo: Por cada factor se ha determinado ciertos criterios que permitan evaluarlo de una forma más objetiva y limitando la subjetividad. Dichos criterios (peso asignado), consideran la frecuencia y la materialidad de dichos factores. La evaluación del nivel de riesgo presenta ponderaciones de entre 1 y 5, siendo 1 riesgo bajo, 3 riesgo moderado y 5 riesgo alto; la ponderación cero (0) corresponde al cumplimiento cabal de los controles. Los factores de riesgo que no son aplicables en la categoría específica se deben dejar en blanco, a fin de no distorsionar el promedio del factor.

Ponderación de Riesgo: Es el porcentaje asignado a cada factor de riesgo de acuerdo a la importancia del Riesgo Inherente y de Control. La importancia se establece asignando porcentajes del 0 al 100 por ciento, de manera que la suma de estos puntajes de importancia sea igual a 100.

Riesgo ponderado calculado: Corresponde al puntaje del factor de riesgo multiplicado por el peso porcentual de la ponderación de riesgo. La suma del riesgo ponderado calculado de los factores va desde 0 a 5.

Ratio del Riesgo Inherente: Es la sumatoria del riesgo ponderado calculado de los riesgos inherentes en los cuales se ha considerado los rangos que determinan el nivel de riesgo: hasta 5 Riesgo Bajo; entre 6 y 10 Riesgo Moderado; y, Alto mayor a 10. El máximo ratio es 15.

Ratio del Riesgo de Control: Es la sumatoria del riesgo ponderado calculado de los riesgos de control en los cuales se ha considerado los rangos que determinan el nivel de

control interno en el área evaluada: hasta 5 Riesgo Alto; entre 6 y 10 Riesgo Moderado; y, mayor a 10 Bajo, siendo el máximo ratio 20.

Total Ratio de Riesgo Agregado: Es la sumatoria del ratio del riesgo inherente y de control en los cuales se ha considerado los rangos que determinen el nivel de riesgo del proceso donde: hasta 11 Riesgo Bajo; entre 12 y 21 Riesgo Moderado; y, Alto mayor a 22. Siendo el máximo ratio es 35.

Descripción de los Factores que intervienen en la Matriz

FACTORES DE RIESGO INHERENTE

Riesgo Inherente, Este tipo de riesgo tiene que ver exclusivamente con la actividad económica o negocio de la empresa, independientemente de los sistemas de control internos que allí se estén aplicando, los Riesgos están presentes en cualquier sistema o proceso que se ejecute.

El riesgo inherente es propio de toda actividad de los procesos, que no puede ser eliminados del sistema, es la posibilidad de que ocurran errores o irregularidades significativos, sin considerar el efecto del control interno, surgen de la exposición o incertidumbre de probables eventos o cambios en las condiciones del negocio o economía que pueden impactar la actividad.

A. *Complejidad y tamaño de la Operación*

Complejidad de la Operación

Las posibilidades de incremento de riesgo y error en el procesamiento dependen en gran medida de la complejidad de las operaciones. Los factores que inciden en la complejidad, entre las más importantes, son: el número de subprocesos que intervienen; las diferentes

áreas que participan; contratación de servicios externos (proveedores); y, complejidad en las actividades (tareas simples y/o especializadas) en la ejecución del proceso.

Grado de automatización

Corresponde a la relación entre el número de operaciones procesadas automáticamente mediante los diferentes aplicativos tecnológicos y las operaciones manuales. Una mayor presencia de procesos manuales incrementa las posibilidades de error y fraude. El análisis del grado de automatización incluye el número de aplicativos tecnológicos que intervienen en el proceso y los cambios importantes en la tecnología, y nivel de obsolescencia.

Registro contable de las operaciones

Corresponde al registro contable de las operaciones por su frecuencia y parametrización tomando en cuenta si son rutinarias y no rutinarias. Las transacciones no rutinarias por ser de naturaleza no recurrentes y esporádicas, conllevan a mayor probabilidad de presencia de errores.

B. *Naturaleza del Entorno de Negocios*

Complejidad de leyes y regulaciones

Aspectos legales y regulatorios (leyes, reglamentos, resoluciones, entre otros) de organismos de control que afectan a los procesos y la complejidad de su aplicación. Mientras más compleja es la normativa legal se demanda más apoyo del criterio de un especialista, tiempo, presupuesto, tecnología, e implementación de controles.

Historia de pérdidas por fraude y errores externos

Corresponde a las pérdidas ocasionadas por fraudes y errores externos generados por terceros y que pueden tener relación con los principales riesgos inmersos en el proceso

analizado; así mismo, fallas en el servicio de proveedores por incumplimiento de niveles de servicio que originan reclamos de clientes. La ponderación para los fraudes, robos y asaltos se obtiene conforme el valor en exposición (pérdida neta) en relación a la materialidad establecida para el proceso/cuenta.

C. Naturaleza Interna de la Entidad

Historia de pérdidas por fraude y errores internos

Corresponde a las pérdidas de años anteriores o en el actual, ocasionadas por fraudes y errores internos que pueden ser por debilidades en el control interno o fallas en el cumplimiento de políticas y procedimientos dentro de la Institución financiera, que están relacionados con el proceso analizado e involucramiento con empleados o funcionarios de la entidad. El historial se puede obtener de la estadística de fraudes de la Unidad de Atención al cliente de la Institución Financiera.

Rotación de Personal

La rotación de personal se define como la fluctuación de personal entre una organización y su ambiente, en el cual se evalúa si esta es adecuada o si ha existido una rotación excesiva del personal gerencial, de supervisión u operativo que ejecuta el proceso. Adicionalmente, se debe tomar en cuenta los planes de sucesión y backups para cubrir y controlar posibles ausencias o salidas del personal.

Comisiones

Inadecuados planes de evaluación y compensación salarial, pueden ejercer presiones sobre los funcionarios para manipular las cifras u ocultar circunstancias que afecten su evaluación. La existencia en sí de estos planes, no significa necesariamente que las operaciones van a ser distorsionadas; sin embargo, incrementan las posibilidades de este hecho. Inciden desfavorablemente: la asignación de metas irreales, excesivamente agresivas; planes estándar sin considerar situaciones particulares; falta de validación de los

planes de compensación. En adición, planes inadecuados de compensación, metas irreales; pueden ocasionar desmotivación del personal, por lo tanto, baja productividad; y, extremamente, incrementar las posibilidades de cometimiento de fraude.

FACTORES DE RIESGO DE CONTROL

Riesgo de Control: Aquí influye de manera muy importante los sistemas de control interno que estén implementados en la Institución Financiera y que a pesar de estos no se pueda detectar o evitar errores o irregularidades significativos en forma oportuna. Debido a esto la necesidad y relevancia que una administración tenga en constante revisión, verificación y ajustes a los procesos de control interno.
Entre los factores relevantes que determina este tipo de riesgo son los sistemas de información, contabilidad y control.
La existen de procedimientos y un adecuado sistema de control puede ayudar a mitigar el riesgo inherente.

Cumplimiento de políticas y procedimientos

Diseño e implementación de políticas y procedimientos

El manual de procedimientos es un documento que contiene la descripción de actividades que deben seguirse en la realización de las funciones de un proceso en donde se debe incluir las políticas que norman la ejecución de los procedimientos.

El diseño e implementación de las políticas y procedimientos es encargada la administración de la Institución Financiera, las cuales se incluyen en los manuales de cada proceso; y, el Directorio es quien revisa y aprueba estos manuales.

Adecuadas y claros niveles de autorización

El manual de funciones es un documento donde se describen las normas y tareas que desarrolla cada funcionario en sus actividades cotidianas y es elaborado técnicamente basado en procedimientos, sistemas, normas que resumen el establecimiento de guías y orientaciones para desarrollar las rutinas o labores diarias. Estos manuales deben ser actualizados cada vez que existan reingeniería de procesos.

Entre los aspectos más significativos a tener en cuenta a la hora de establecer la estructura organizativa correspondiente están la definición de las áreas clave de autoridad y responsabilidad y el establecimiento de niveles de autorización.

Cumplimiento de leyes y reglamentos relevantes por parte del personal clave

El error u omisión en el cumplimiento de aspectos legales e impositivos, pueden representar multas y sanciones al personal clave y/o la entidad financiera; y, dependiendo de la ley, reglamento o norma que se puede incumplir, podría en casos extremos influir en la continuidad de las operaciones de la entidad financiera.

Es importante mencionar que este tipo de incumplimientos puede conducir a riesgo reputacional, cuyos efectos pueden ser de mayor gravedad a las mismas multas y sanciones.

Nivel de cumplimiento con políticas y procedimientos relevantes por parte del personal clave

El personal clave debe conocer las políticas y procedimientos de los procesos para que exista un adecuado control y cumplimiento de los mismos y de esta forma apoyar las estrategias y objetivos institucionales.

Estructura y eficacia del control interno

Es el elemento que proporciona disciplina y estructura. El ambiente de control se determina en función de la integridad y competencia del personal de una organización; los valores éticos son un elemento esencial que afecta a otros componentes del control.

Reportes para el monitoreo de las operaciones

Es fundamental para el monitoreo de las operaciones la existencia de reportes que ayuden al personal a controlar la adecuada ejecución y funcionamiento de los procesos (cumplimiento de los controles implantados), los procedimientos para el monitoreo deben estar definidos formalmente en manuales o instructivos con sus respectivos responsables.

Apropiados niveles de supervisión y revisión

Con el fin de reducir el riesgo de que se cometan errores, irregularidades o fraudes, las tareas se distribuyen entre los empleados. Así, por ejemplo, se separan las responsabilidades de autorizar transacciones, de registrarlas y de gestionar los activos correspondientes. Es importante que exista una descripción de funciones por escrito, que se separen funciones incompatibles y que en caso de que existan estas últimas existan controles mitigantes.

Un proceso se mantiene con un adecuado funcionamiento del sistema a lo largo del tiempo cuando se consigue eficiencia mediante actividades de supervisión continua, evaluaciones periódicas con una combinación de ambas cosas.

Adicionalmente se debe considerar que las funciones de supervisión y revisión son conforme a su nivel jerárquico y estos responsables de las diferentes áreas son los encargados de impulsar, coordinar y controlar que todas las actuaciones llevadas a cabo en sus diferentes áreas siguen las directrices establecidas por la administración de la Institución Financiera.

Conocimiento y habilidades del personal

El conocimiento y habilidades del personal involucran el perfil profesional, experiencia y existencia de planes de capacitación.

El perfil profesional encierra las capacidades y competencias de la formación de una persona (experiencia) para asumir en condiciones óptimas las responsabilidades propias del desarrollo de funciones y tareas.

Así, mismo en búsqueda de mejorar la actitud, conocimiento, habilidades y conducta del personal en sus puestos de trabajo se debe tomar en cuenta la existencia de planes de capacitación.

Adecuados controles físicos para evitar el acceso a datos, operaciones y áreas restringidas
La naturaleza de las actividades de la entidad, así como el nivel de acceso del personal a los activos, pueden ser causas de apropiación indebida de los recursos.

Se deben considerar los siguientes tipos de control:

- Controles duales en cajas y bóvedas
- Cajas fuertes para custodia de efectivo (procesos relacionados en sucursales)
- Sistema de archivo de documentos relevantes en cajas de seguridad
- Controles de acceso a áreas de la Institución Financiera, tanto a funcionarios como a personas externas.
- Sistemas de seguridad (alarmas, monitoreo de entrada y salida) sistemas automáticos que capturan el ingreso/salida de personas y son efectivos.
- Seguridades de los sistemas informáticos: perfiles de acceso conforme a funciones, usuarios autorizados, logs de auditoría para validar el registro de transacciones, usuarios genéricos

Grado de implantación de recomendaciones de auditorías anteriores /Frecuencia de hallazgos en auditorias o exámenes anteriores

Está relacionado con el número de observaciones no regularizadas y su nivel de riesgo (alto, moderado y bajo); se debe considerar también el impacto material de dichos incumplimientos. Otro aspecto que tomamos en cuenta, es la recurrencia de que un hallazgo se repite a través de los exámenes de auditoría, lo cual evidencia que no se

tomaron los correctivos y que a pesar que se pudo haber corregido, los mismos vuelven a presentarse en una nueva revisión.

Calidad e Integridad de la Información Financiera e Información Gerencial

Adecuados sistemas de información gerencial

Es determinar si los sistemas y/o aplicativos que intervienen en el proceso son adecuados y emiten reportes gerenciales automáticos o deben realizarse manualmente, y que dichos reportes permitan determinar adecuados controles y la toma de decisiones oportunas; facilitando conciliaciones periódicas.

Integridad de las fuentes de información

Corresponde a la seguridad de las bases de datos o fuente de información que son parte del proceso, la medida en que las mismas pueden ser objeto de manipulación intencionada.

Revisión independiente y conciliación de la información

Evaluar si las revisiones que se realiza en las diferentes etapas del proceso (reportes y/o documentos) son ejecutadas por personas independientes que no tienen ninguna relación con el proceso analizado y la frecuencia con la que la realizan es adecuado y oportuno (diaria, semanal, mensual, dependiendo la naturaleza de cada proceso), y en caso de presentarse diferencias en las conciliaciones estas son regularizadas de forma oportuna.

D. Efectividad de la Gerencia

Efectividad de la gerencia (monitoreo y control)
La gerencia conoce satisfactoriamente sobre los aspectos importantes del proceso a su cargo, así como los riesgos que pueden afectarlo; investiga y monitorea continuamente (fuentes internas y externas) sobre las condiciones de riesgo que afectan a la organización y

a su proceso. En forma periódica solicita la actualización de los manuales de procedimientos, conforme los nuevos requerimientos del proceso.

Conocimiento, experiencia y habilidad

El conocimiento y habilidades de la gerencia (responsables y jefaturas) involucran el perfil profesional (formación académica, experiencia en el cargo o funciones similares, conocimientos, destrezas y habilidades) para asumir en condiciones óptimas las responsabilidades propias del desarrollo de funciones y tareas.

Adecuada supervisión

Una adecuada supervisión incluye frecuencia y oportunidad de la supervisión aplicada, existencia de comunicaciones por escrito sobre instrucciones y correctivos; y, seguimiento al cumplimiento oportuno y adecuado de las decisiones e instrucciones emitidas.

Adecuada comunicación de la gerencia

La gerencia debe estar muy atenta cómo se maneja la comunicación, y desde luego, como la está difundiendo a fin usarla adecuadamente, se obtenga un clima armónico, con resultados positivos. La información y decisiones relevantes deben ser comunicadas oportunamente y por escrito a los funcionarios claves, facilitándoles asumir sus responsabilidades individuales y el compromiso de apoyo al logro de los objetivos y estrategias de la organización.

Uso de reportes gerenciales para medir y monitorear

La utilización de reportes gerenciales adecuados facilita el monitoreo de las operaciones y el cumplimiento de los controles implantados y la toma oportuna de decisiones. Otra herramienta eficiente, es el manejo de presupuestos para la evaluación financiera del área. Adicionalmente, se debe considerar que las decisiones y definiciones tomadas en comités o

juntas (reuniones) deben sustentarse en actas formales (firmadas, foliadas, enumeradas y archivadas) para un posterior seguimiento y cumplimiento.

3.2.6. Evaluación de los procesos en base a la Matriz de Factores del Riesgo de Auditoría

En base al Universo Auditable se ejemplificará la aplicación de la Matriz en dos procesos:

3.2.6.1. Aplicación de la Matriz – Ejemplo 1

Tabla 13:

Matriz Detallada de Factores de Riesgo – Proceso 1 (Transporte de Valores)

Factores de Riesgo	Puntaje del Factor de Riesgo	Explicación de Evaluación
FACTORES DE RIESGO INHERENTE		
A. Complejidad y tamaño de la Operación		
Complejidad de la Operación	4,75	
Subprocesos que intervienen en el proceso	5	1 : hasta 1 subprocesos 2: hasta 2 subprocesos 3: hasta 3 subprocesos 4: hasta 4 subprocesos 5: más de 5 subprocesos
Áreas que participan en el proceso	5	1 : una sola área 2 - 3 : 2 a 3 áreas 4 - 5: más de 3 áreas
Participación de proveedores externos (empresas de servicios)	5	0: sin intervención 1 : Participa en el proceso una empresa 2: Participa en el proceso dos empresas 3: Participan en el proceso más de tres empresas Entre 1 y 2 puntos adicionales por mala experiencia con los proveedores (niveles de servicio)
Complejidad en las actividades / procedimientos en la ejecución	4	1 : Tareas simples y no especializadas 2 - 3 : La actividad requiere varias tarea especializadas

Factores de Riesgo	Puntaje del Factor de Riesgo	Explicación de Evaluación
del proceso		(requiere criterio) y la interacción de varias personas 4 - 5 : Varios tareas especializadas que requieren coordinación de varias personas en el proceso y con otros procesos.
Grado de automatización	4	
Número de aplicativos tecnológicos que intervienen en el proceso	5	1 : un solo aplicativo 2 : 2 aplicativos 3 - 5 : más de 2 aplicativos que intervienen en el proceso
Número de operaciones automatizadas y/o manuales	4	0 : sin operaciones manuales (100% operaciones automáticas) 1 : hasta 10% del total de operaciones manuales. 2 - 3: entre el 11% y el 25% de operaciones manuales 4 - 5: más del 25%
Cambios importantes en la tecnología y nivel de obsolescencia	3	0 : Sin cambios en los últimos 12 meses 1 : Con cambios en los últimos 12 meses 2 - 3: Algunos cambios en la tecnología (sistemas) con cierto impacto en los últimos 12 meses. 4 : Cambios importante en el negocio o en el proceso o nuevo sistema de tecnología en los últimos 12 meses. 5 : Obsolescencia de aplicativos tecnológicos.
Registro contable de las operaciones	2	
Registro contable de las operaciones (frecuencia versus parametrización).	2	1 - 2: operaciones donde en registro contable el rutinario y parametrizado. 3- 4: operaciones donde el registro contable es rutinario y no parametrizado. 5: operaciones donde el registro contable no es rutinario y no parametrizado.
B. Naturaleza del Entorno de Negocios		
Complejidad de leyes y regulaciones.	4	
Normativa legal y su complejidad en los procesos	4	0 - 1: Normativa legal no compleja 2 - 3: Alguna normativa legal con cierta complejidad 4 - 5: Cantidad importante de normativa legal y muy

Factores de Riesgo	**Puntaje del Factor de Riesgo**	**Explicación de Evaluación**
		compleja
Historia de pérdidas por fraude y errores externos	1	
Fraudes, robos y asaltos	0	Se obtiene conforme el valor en exposición (pérdida neta) en relación la materialidad establecida para el proceso/cuenta (pérdida neta/materialidad *5)
Fallas en el servicio de proveedores (Incumplimiento de niveles de servicio) que originaron reclamos de clientes (incluido fraude)	2	0 - 1: Eventuales reclamos de clientes de insignificante valor material en los últimos 12 meses 2 - 3: Eventuales reclamos de clientes de valor material importante en los últimos 12 meses 4 - 5: Continuos reclamos de clientes de valor importante en los últimos 12 meses (considerar la materialidad establecida para el proceso)
C. Naturaleza Interna de la Entidad		
Historia de pérdidas por fraude y errores internos	1,7	
Fraudes informáticos	0	0 - 1: Sin historial importante en número y monto 2 - 3: Varios casos de fraude, debilidad del Control Interno o fallas en el cumplimiento de políticas y procedimientos pero no de gran importancia en los últimos 12 meses. 4 - 5: Debilidades del Control Interno o fallas en el cumplimiento de políticas y procedimientos de gran importancia en los últimos 12 meses, que originaron fraude interno.
Fraudes cometidos por el personal del Banco	1	0 - 1: Sin historial importante en número y monto 2 - 3: Varios casos de fraude, debilidad del Control Interno o fallas en el cumplimiento de políticas y procedimientos pero no de gran importancia en los últimos 12 meses. 4 - 5: Debilidades del Control Interno o fallas en el cumplimiento de políticas y procedimientos de gran importancia en los últimos 12 meses, que originaron fraude interno.
Error u omisión en la ejecución de los procesos	4	0 - 1: Sin historial importante en número y monto 2 - 3: Varios casos de errores u omisiones en la ejecución del proceso pero no de gran importancia en los últimos 12 meses.

Factores de Riesgo	Puntaje del Factor de Riesgo	Explicación de Evaluación
		4 - 5: Varios casos de errores u omisiones en la ejecución del proceso de gran importancia en los últimos 12 meses, que originaron pérdidas económicas para la entidad financiera.
Rotación de Personal	2,3	
Rotación de personal clave y niveles de supervisión	2	0: sin rotación en los últimos 12 meses de los funcionarios 1-2: salida del supervisor 3-4: salida del responsable 5 : salida del vicepresidente
Alta rotación del personal operativo	3	Corresponde al porcentaje de rotación del personal del área auditada, (Porcentaje de Rotación*5). Información que debe ser solicitada a la Unidad de RRHH.
Planes de sucesión y backups	2	0 : Existencia de planes de sucesión y backups. 1 - 2: Planes de sucesión y backups incompletos hasta el 50% 3 - 4 : Planes de sucesión y backups incompletos más del 50% 5 : Falta de planes de sucesión y backups
Comisiones del personal	1	
Incentivo adicional a la remuneración básica	1	0 : no existen comisiones 1 - 2: comisiones sin efecto importante (hasta el 5%) 3 - 4: comisiones entre el 6% y el 20% 5 : las comisiones son mayores del 21% al 30% en relación con la remuneración.
FACTORES DE RIESGO DE CONTROL		
A. Cumplimiento de políticas, procedimientos y normativa legal		
Diseño e implementación de políticas y procedimientos	0	
Existencia de manuales (políticas y procedimientos por escrito) y que se encuentran aprobadas	0	0 : Existen manuales aprobador por el Directorio 1 - 2: Existen manuales actualizados sin aprobación del Directorio 3 -4 : Manuales en proceso de elaboración que no están revisados ni aprobados

Factores de Riesgo	Puntaje del Factor de Riesgo	Explicación de Evaluación
		5 : No existen manuales.
Adecuadas y claros niveles de autorización	0	
Existencia de manual de funciones	0	0 : Existencia de manuales de funciones actualizados 1 - 2: Las funciones se encuentran desactualizadas en manuales, pero no existe mayor incidencia en los procesos. 3 -4 : Las funciones se encuentran desactualizadas en manuales y existe importante incidencia en los procesos 5 : No existen manuales de funciones
Existencia de adecuados niveles de autorización	0	0 : Existen niveles de autorización aprobados 1 - 3: Existen niveles de autorización no aprobados 4 - 5: No existen niveles de autorización
Cumplimiento de leyes y reglamentos relevantes por parte del personal clave	1	
Multas y sanciones por el no cumplimiento de regulaciones de entes de control	1	0 : No existencia de sanciones y multas para el personal clave y/o la entidad financiera. 1 - 2: Multas para el personal clave y/o la entidad financiera. 3 - 4: Posibilidad de destitución de personal clave 5 : Posibilidad de cierre temporal de las operaciones en sucursales y/o la entidad financiera.
Nivel de cumplimiento con políticas y procedimientos relevantes.	3	
Nivel de cumplimiento de políticas y procedimientos por parte del personal clave.	3	0 - 1: No existe incumplimiento del personal clave 2 - 3: Incumplimiento de políticas y procedimientos por funcionarios claves que no afectan significativamente el proceso 4 - 5: Incumplimiento de varias políticas y procedimientos por funcionarios claves que afectan significativamente el proceso
B. Estructura y Eficacia del Control Interno		

Factores de Riesgo	Puntaje del Factor de Riesgo	Explicación de Evaluación
Reportes para el monitoreo de las operaciones	1	
Existencia de reportes para monitorear las operaciones.	1	0 : Existen definidos reportes, procedimientos formales y funcionarios responsables para el monitoreo. 1 -2: Existen reportes, y monitoreo no frecuente y no se han definido procedimientos ni funcionarios responsables. 3 -4: Existen reportes, no se realizan monitoreo y no se han definido funcionarios responsables. 5 : No existen reportes, procedimientos y tampoco se han definido funcionarios responsables.
Apropiados niveles de supervisión y revisión	1,5	
Adecuada segregación de funciones	1	0 : Existe adecuada segregación de funciones. 1 : Algunas actividades que no afectan significativamente el proceso, no tienen una adecuada segregación de funciones 2-3: Gran parte de las actividades que pueden afectar significativamente al proceso no se encuentran segregadas. 4-5: Ausencia total de segregación de funciones.
Evidencia de revisión y supervisión	2	0 : Existe evidencia de supervisión 1 - 2: Existe supervisión pero no existe una adecuada evidencia. 3 - 4 : No existe supervisión y evidencia en procedimientos significativos. 5 : No existe supervisión
Conocimiento y habilidades del personal	1,3	
Personal del área cumple con el perfil requerido para el cargo	1	0 : Personal cumple con el perfil requerido para los diferentes cargos 1 - 3: Personal cumple parcialmente con el perfil requerido para los cargos. 4 - 5: Personal no cumple con el perfil requerido para los cargos asignados.
Experiencia en el desempeño de funciones	1	0 - 1: Desempeño de funciones en el cargo mayor a tres años y demuestra efectividad y eficiencia. 2 - 3: Desempeño entre 1 y 3 años en las funciones y su efectividad y eficiencia están en proceso de afianzamiento. 4 : Desempeño de las funciones o cargos similares hasta

Factores de Riesgo	Puntaje del Factor de Riesgo	Explicación de Evaluación
		un año. 5 : Sin experiencia en el cargo o funciones similares.
Existencia de planes de capacitación	2	0 : El personal ha recibido capacitación formal (interna o externa) con respecto a las políticas y procedimientos, aspectos legales, relacionados con el cargo, en los últimos 12 meses; o, no han existido cambios relevantes en sus funciones. 1 - 3: El personal ha recibido capacitación formal con respecto a sus funciones, en un tiempo mayor a 12 meses. 5 : No existe capacitación ni un plan anual.
Adecuados controles físicos para evitar el acceso a datos, operaciones y áreas restringidas	1,2	
Controles duales en cajas y bóvedas	0	0 : Se cumplen con los controles duales. 5: No se cumplen con los controles duales.
Cajas fuertes para custodia de efectivo (procesos relacionados en sucursales)	3	0 : Existen y se utilizan cajas fuertes 5: No existen o no se utilizan cajas fuertes
Sistema de archivo de documentos relevantes	3	0 : Archivo adecuado de documentación relevante en cajas de seguridad 1 -2 : Sistema de archivo físico no es caja de seguridad, pero brinda salvaguarda adecuada. 3 - 4: Los documentos relevantes se resguardan en un archivador simple sin acceso restringido. 5 : El sistema de archivo no brinda ningún tipo de seguridad.
Controles de acceso a áreas de la Institución, tanto a funcionarios como a personas externas.	0	0 : Existen sistemas automáticos que capturan el ingreso/salida de personas y son efectivos. 1 - 2: El control de acceso se realiza mediante bitácoras manuales y las mismas son validadas por parte de un funcionario independiente en forma periódica. 3 - 4: Existen sistemas automáticos/manuales; sin embargo, no funcionan y/o no cuentan con monitoreo adecuado. 5 : No existen sistemas automáticos ni manuales para el control de acceso.
Sistemas de seguridad (alarmas, monitoreo de entrada y salida)	0	0 : Existen sistemas de seguridad: alarmas, monitoreo de entrada y salida, cámaras y guardianía (de ser necesario). 1 - 2: Existen sistemas de seguridad: alarmas, monitoreo de entrada y salida, no existen cámaras ni vigilancia armada

Factores de Riesgo	**Puntaje del Factor de Riesgo**	**Explicación de Evaluación**
		(guardias). 3 - 4: Los sistemas han presentado deficiencias. 5 : No existen sistemas de seguridad.
Seguridades de los sistemas informáticos	1	Considerar: a. Perfiles de acceso están conforme a funciones b. Presencia de usuarios autorizados. c. Existencia de logs de auditoría (rastro de las transacciones) d. Inexistencia de usuarios genéricos ---------- 0-1 : Cumplimiento de a),b), c), d). 2 : Cumple al menos 3 de los factores 3 : Cumple al menos 2 de los factores. 4 - 5: No cumple ninguno de estos factores.
Grado de implementación de recomendaciones de auditorías anteriores	1,5	
Observaciones no regularizadas de anteriores auditorías	1	0: Todas las observaciones de Auditorías anteriores fueron implementadas 1: hasta el 5% de observaciones 2: entre 6% y 15% 3: más del 15%. Un punto adicional para observaciones de Riesgo Moderado y dos puntos para las de Riesgo Alto
Reincidencia de las observaciones no regularizadas (Se refiere a observaciones que fueron regularizadas pero su incumplimiento se convirtió en recurrente).	2	1: hasta el 5% de observaciones de la presente revisión son reincidentes 2: entre 6% y 15% 3: más del 15%. Un punto adicional para observaciones de Riesgo Moderado y dos puntos para las de Riesgo Alto.
C. *Calidad e Integridad de la Información Financiera e Información Gerencial.*		
Adecuados sistemas de información gerencial	3	

Factores de Riesgo	**Puntaje del Factor de Riesgo**	**Explicación de Evaluación**
Los sistemas que intervienen en el proceso, emiten reportes gerenciales	4	0 : El sistema emite reportes gerenciales y son utilizados por el personal clave. 1 - 3: El sistema emite reportes gerenciales y no son utilizados por el personal clave 4 - 5: El sistema no emite reportes gerenciales
Emisión de reportes (automáticos y manuales)	2	0 : Todos los reportes son automáticos 1 -2: Los reportes manuales corresponden a un 25% de la información relevante. 3 -4 : Los reportes manuales corresponden hasta un 50% de la información relevante. 5 : Más del 50% de los reportes son manuales.
Integridad de las fuentes de información	2	
Integridad de las bases de datos	2	0: Las bases de datos que intervienen en el proceso, provienen de sistemas cerrados, en los cuales no es posible la manipulación. 5: Las bases de datos que intervienen en el proceso, no provienen de sistemas cerrados y/o es posible la manipulación.
Revisión independiente y conciliación de la información	3	
Frecuencia de la conciliación de la información	3	0 : Se realiza una conciliación frecuente y oportuna (diaria, semanal, mensual, etc., dependiendo de la naturaleza de cada proceso) 1 - 2: Los reportes se concilian pero presentan diferencias inmateriales. 3 - 4: Se realiza una conciliación de manera esporádica y las diferencias son importantes y no regularizadas 5 : No se realizan conciliaciones de la información.
D. Efectividad de la Gerencia		
Efectividad de la gerencia (monitoreo y control)	2	
La gerencia investiga y monitorea continuamente (fuentes internas y externas) sobre los riesgos que afectan a la organización y a su	3	0 : Existe un sistema/procedimiento formal debidamente aprobado para la investigación y monitoreo de riesgos, el cual se aplica sistemáticamente. 1 -2: Existe un sistema/procedimiento formal para la investigación y monitoreo de riesgos, sin embargo su

Factores de Riesgo	Puntaje del Factor de Riesgo	Explicación de Evaluación
proceso		aplicación ha alcanzado máximo un 75% del total del proceso/cuenta. 3 -4 : Existe un sistema/procedimiento formal para la investigación y monitoreo de riesgos, sin embargo es obsoleto o insuficiente para su propósito final. 5 : No existe un sistema de investigación ni monitoreo de riesgos.
La gerencia actualiza los manuales de procedimientos conforme los nuevos requerimientos del proceso (riesgo y controles), en forma oportuna.	1	0 : La actualización de manuales es inmediata, conforme a los cambios del proceso (máximo 30 días). 1 -2: La actualización de manuales es mediata, conforme a los cambios del proceso (máximo 60 días). 3 -4 : La actualización de manuales es tardía, frecuencia mayor a 60 días. 5 : No existe actualización de manuales, conforme los cambios del proceso.
Conocimiento, experiencia y habilidad	1,5	
Perfil profesional conforme funciones	2	0 : El perfil profesional de la gerencia corresponde con las funciones asignadas 1 - 3: El perfil profesional corresponde parcialmente con los requerimientos del cargo. 4 - 5: El perfil no está de acuerdo con las funciones que desempeña y son totalmente diferentes al perfil del puesto.
Experiencia profesional	1	0 - 1: Experiencia mayor a tres años y demuestra efectividad y eficiencia en el cargo. 2 - 3: Experiencia entre 1 y 3 años en las funciones y su efectividad y eficiencia están en proceso de afianzamiento. 4 : Experiencia profesional hasta un año en las funciones que desempeña o en cargos similares. 5 : Sin experiencia en el cargo o funciones similares.
Adecuada supervisión	1	
Frecuencia y oportunidad de la supervisión	1	0 : Evidencia de supervisión continua y oportuna y seguimiento a instrucciones. 1 - 2: Evidencia de supervisión; sin embargo, las principales decisiones tomadas, no se han implantado en forma oportuna y adecuada. 3 - 4: Supervisión no regular. 5 : No existe supervisión.

Factores de Riesgo	Puntaje del Factor de Riesgo	Explicación de Evaluación
Adecuada comunicación de la gerencia	3	
Comunicación de la información oportuna	3	0 : La transmisión de información relevante es oportuna y por escrito. 1 - 3: La información se comunica en forma verbal y se efectúan comunicaciones por escrito con cierta demora (hasta una semana). 4 - 5: No existe evidencia de transmisión de información y decisiones relevantes.
Uso de reportes gerenciales para medir y monitorear	4,3	
Utilización de reportes que faciliten el monitoreo de las operaciones y el cumplimiento de los controles implantados.	4	0 : Utilizan reportes únicamente automatizados para el monitoreo y supervisión de las operaciones; adicionalmente, éstos arrojan alertas a través de la cuales se pueden implementar mejores controles. 1 - 2: Utilizan reportes manuales y automatizados para el monitoreo y supervisión de las operaciones. 3 - 4: No se han incluido en el sistema de reportes todos los informes necesarios para toma de decisiones. 5 : No utilizan reportes para el monitoreo de las operaciones.
Utilización de presupuestos para evaluación	4	0 : Se realizan evaluaciones mensuales del presupuesto. 1 - 2: Las evaluaciones presupuestarias se efectúan por períodos mayores a un mes (hasta 3 meses). 3 - 4: El análisis presupuestario se realiza en forma esporádica (mayor a 3 meses). 5 : El área no realiza evaluaciones periódicas del presupuesto o no existe presupuesto.
Existencia de comités o juntas. Se emiten actas donde se resumen las principales decisiones.	5	0 : Existen actas de los comités donde se incluyen las decisiones tomadas y éstas se encuentren debidamente foliadas, enumeradas y con las firmas respectivas y archivadas adecuadamente. 1 - 3: Las actas se oficializan vía e-mail entre los asistentes a los comités, sin embargo, no se mantiene un control del archivo (electrónico o físico) de dichas comunicaciones. 4 - 5: Los comités no formalizan las decisiones mediante actas o algún documento similar.

Tabla 14:

Matriz Resumen de Factores de Riesgo – Proceso 1 (Transporte de Valores)

Factores de Riesgo	Puntaje del Factor de Riesgo	Ponderación de Riesgo	Riesgo ponderado calculado
FACTORES DE RIESGO INHERENTE			
A. Complejidad y tamaño de la Operación			
Complejidad de la Operación	4,75	40%	1,9
Grado de automatización	4	30%	1,2
Registro contable de las operaciones	2	30%	0,6
Subtotal		100%	3,7
B. Naturaleza del Entorno de Negocios			
Complejidad de leyes y regulaciones.	4	60%	2,4
Historia de pérdidas por fraude y errores externos	1	40%	0,4
Subtotal		100%	2,8
C. Naturaleza Interna de la Entidad			
Historia de pérdidas por fraude y errores internos	1,7	40%	0,67
Rotación de Personal	2,3	30%	0,70
Comisiones del personal	1,0	30%	0,30
Subtotal		100%	1,67
TOTAL RATIO DE RIESGO INHERENTE		**Moderado**	**8**
FACTORES DE RIESGO DE CONTROL			
A. Cumplimiento de políticas, procedimientos y normativa legal			
Diseño e implementación de políticas y procedimientos	0	25%	0

Factores de Riesgo	Puntaje del Factor de Riesgo	Ponderación de Riesgo	Riesgo ponderado calculado
Adecuadas y claros niveles de autorización	0	25%	0
Cumplimiento de leyes y reglamentos relevantes por parte del personal clave	1	25%	0,25
Nivel de cumplimiento con políticas y procedimientos relevantes.	3	25%	0,75
Subtotal		100%	1
B. Estructura y Eficacia del Control Interno			
Reportes para el monitoreo de las operaciones	1	20%	0,2
Apropiados niveles de supervisión y revisión	1,5	20%	0,3
Conocimiento y habilidades del personal	1,33	20%	0,27
Adecuados controles físicos para evitar el acceso a datos, operaciones y áreas restringidas	1,17	20%	0,23
Grado de implementación de recomendaciones de auditorías anteriores	1,5	20%	0,3
Subtotal		100%	1,3
C. *Calidad e Integridad de la Información Financiera e Información Gerencial.*			
Adecuados sistemas de información gerencial	3	30%	0,9
Integridad de las fuentes de información	2	30%	0,6
Revisión independiente y conciliación de la información	3	40%	1,2
Subtotal		100%	2,7
D. Efectividad de la Gerencia			
Efectividad de la gerencia (monitoreo y	2	20%	0,4

Factores de Riesgo	Puntaje del Factor de Riesgo	Ponderación de Riesgo	Riesgo ponderado calculado
control)			
Conocimiento, experiencia y habilidad	1,5	20%	0,3
Adecuada supervisión	1	20%	0,2
Adecuada comunicación de la gerencia	3	20%	0,6
Uso de reportes gerenciales para medir y monitorear	4,33	20%	0,87
Subtotal		100%	2,37
TOTAL RATIO DE RIESGO DE CONTROL		**Moderado**	**7,37**
TOTAL RATIO DE RIESGO AGREGADO		**Moderado**	**15,53**

Resultado: En la evaluación del proceso de Transporte de Valores podemos concluir que este proceso mantiene un riesgo inherente moderado; siendo el factor de riesgo más relevante de la complejidad y tamaño de la operación debido al core del proceso en sí mismo a la complejidad, grado de automatización y registro contable, ya que el transporte de efectivo encierra actividades especializadas y sensitivas dentro de la institución. Adicionalmente, este proceso mantiene un riesgo de control moderado, lo cual indica que tiene los controles implementados son relativamente tolerables. Concluyendo que este proceso es Riesgo Moderado con un ratio de 15 puntos.

3.2.6.2. Aplicación de la Matriz – Ejemplo 2

Tabla 15:

Matriz Detallada de Factores de Riesgo – Proceso 2 (Corresponsales No Bancarios)

Factores de Riesgo	Puntaje del Factor de Riesgo	Explicación de Evaluación
FACTORES DE RIESGO INHERENTE		

Factores de Riesgo	Puntaje del Factor de Riesgo	Explicación de Evaluación
A. Complejidad y tamaño de la Operación		
Complejidad de la Operación	5	
Subprocesos que intervienen en el proceso	5	1 : hasta 1 subprocesos 2: hasta 2 subprocesos 3: hasta 3 subprocesos 4: hasta 4 subprocesos 5: más de 5 subprocesos
Áreas que participan en el proceso	5	1 : una sola área 2 - 3 : 2 a 3 áreas 4 - 5: más de 3 áreas
Participación de proveedores externos (empresas de servicios)	5	0: sin intervención 1 : Participa en el proceso una empresa 2: Participa en el proceso dos empresas 3: Participan en el proceso más de tres empresas Entre 1 y 2 puntos adicionales por mala experiencia con los proveedores (niveles de servicio)
Complejidad en las actividades / procedimientos en la ejecución del proceso	5	1 : Tareas simples y no especializadas 2 - 3 : La actividad requiere varias tarea especializadas (requiere criterio) y la interacción de varias personas 4 - 5 : Varios tareas especializadas que requieren coordinación de varias personas en el proceso y con otros procesos.
Grado de automatización	3,7	
Número de aplicativos tecnológicos que intervienen en el proceso	3	1 : un solo aplicativo 2 : 2 aplicativos 3 - 5 : más de 2 aplicativos que intervienen en el proceso
Número de operaciones automatizadas y/o manuales	4	0 : sin operaciones manuales (100% operaciones automáticas) 1 : hasta 10% del total de operaciones

Factores de Riesgo	Puntaje del Factor de Riesgo	Explicación de Evaluación
		manuales. 2 - 3: entre el 11% y el 25% de operaciones manuales 4 - 5: más del 25%
Cambios importantes en la tecnología y nivel de obsolescencia	4	0 : Sin cambios en los últimos 12 meses 1 : Con cambios en los últimos 12 meses 2 - 3: Algunos cambios en la tecnología (sistemas) con cierto impacto en los últimos 12 meses. 4 : Cambios importante en el negocio o en el proceso o nuevo sistema de tecnología en los últimos 12 meses. 5 : Obsolescencia de aplicativos tecnológicos.
Registro contable de las operaciones	4	
Registro contable de las operaciones (frecuencia versus parametrización).	4	1 - 2: operaciones donde en registro contable el rutinario y parametrizado. 3- 4: operaciones donde el registro contable es rutinario y no parametrizado. 5: operaciones donde el registro contable no es rutinario y no parametrizado.
B. Naturaleza del Entorno de Negocios		
Complejidad de leyes y regulaciones.	2	
Normativa legal y su complejidad en los procesos	2	0 - 1: Normativa legal no compleja 2 - 3: Alguna normativa legal con cierta complejidad 4 - 5: Cantidad importante de normativa legal y muy compleja
Historia de pérdidas por fraude y errores externos	2	

Factores de Riesgo	Puntaje del Factor de Riesgo	Explicación de Evaluación
Fraudes, robos y asaltos	0	Se obtiene conforme el valor en exposición (pérdida neta) en relación la materialidad establecida para el proceso/cuenta (pérdida neta/materialidad *5)
Fallas en el servicio de proveedores (Incumplimiento de niveles de servicio) que originaron reclamos de clientes (incluido fraude)	4	0 - 1: Eventuales reclamos de clientes de insignificante valor material en los últimos 12 meses 2 - 3: Eventuales reclamos de clientes de valor material importante en los últimos 12 meses 4 - 5: Continuos reclamos de clientes de valor importante en los últimos 12 meses (considerar la materialidad establecida para el proceso)
C. Naturaleza Interna de la Entidad		
Historia de pérdidas por fraude y errores internos	4,5	
Fraudes cometidos por el personal del Banco	4	0 - 1: Sin historial importante en número y monto 2 - 3: Varios casos de fraude, debilidad del Control Interno o fallas en el cumplimiento de políticas y procedimientos pero no de gran importancia en los últimos 12 meses. 4 - 5: Debilidades del Control Interno o fallas en el cumplimiento de políticas y procedimientos de gran importancia en los últimos 12 meses, que originaron fraude interno.
Error u omisión en la ejecución de los procesos	5	0 - 1: Sin historial importante en número y monto 2 - 3: Varios casos de errores u omisiones en la ejecución del proceso pero no de gran importancia en los últimos 12 meses. 4 - 5: Varios casos de errores u omisiones en la ejecución del proceso de gran importancia en los últimos 12 meses, que originaron

Factores de Riesgo	Puntaje del Factor de Riesgo	Explicación de Evaluación
		pérdidas económicas para la entidad financiera.
Rotación de Personal	4	
Rotación de personal clave y niveles de supervisión	4	0: sin rotación en los últimos 12 meses de los funcionarios 1-2: salida del supervisor 3-4: salida del responsable 5 : salida del vicepresidente
Alta rotación del personal operativo	5	Corresponde al porcentaje de rotación del personal del área auditada, (Porcentaje de Rotación*5). Información que debe ser solicitada a la Unidad de RRHH.
Planes de sucesión y backups	4	0 : Existencia de planes de sucesión y backups. 1 - 2: Planes de sucesión y backups incompletos hasta el 50% 3 - 4 : Planes de sucesión y backups incompletos más del 50% 5 : Falta de planes de sucesión y backups
Comisiones del personal	5	
Incentivo adicional a la remuneración básica	5	0 : no existen comisiones 1 - 2: comisiones sin efecto importante (hasta el 5%) 3 - 4: comisiones entre el 6% y el 20% 5 : las comisiones son mayores del 21% al 30% en relación con la remuneración.
FACTORES DE RIESGO DE CONTROL		
A. Cumplimiento de políticas, procedimientos y normativa legal		
Diseño e implementación de	4	

Factores de Riesgo	Puntaje del Factor de Riesgo	Explicación de Evaluación
políticas y procedimientos		
Existencia de manuales (políticas y procedimientos por escrito) y que se encuentran aprobadas	4	0 : Existen manuales aprobador por el Directorio 1 - 2: Existen manuales actualizados sin aprobación del Directorio 3 -4 : Manuales en proceso de elaboración que no están revisados ni aprobados 5 : No existen manuales.
Adecuadas y claros niveles de autorización	3	
Existencia de manual de funciones	3	0 : Existencia de manuales de funciones actualizados 1 - 2: Las funciones se encuentran desactualizadas en manuales, pero no existe mayor incidencia en los procesos. 3 -4 : Las funciones se encuentran desactualizadas en manuales y existe importante incidencia en los procesos 5 : No existen manuales de funciones
Existencia de adecuados niveles de autorización	3	0 : Existen niveles de autorización aprobados 1 - 3: Existen niveles de autorización no aprobados 4 - 5: No existen niveles de autorización
Cumplimiento de leyes y reglamentos relevantes por parte del personal clave	1	
Multas y sanciones por el no cumplimiento de regulaciones de entes de control	1	0 : No existencia de sanciones y multas para el personal clave y/o la entidad financiera. 1 - 2: Multas para el personal clave y/o la entidad financiera. 3 - 4: Posibilidad de destitución de personal clave 5 : Posibilidad de cierre temporal de las

Factores de Riesgo	Puntaje del Factor de Riesgo	Explicación de Evaluación
		operaciones en sucursales y/o la entidad financiera.
Nivel de cumplimiento con políticas y procedimientos relevantes.	3	
Nivel de cumplimiento de políticas y procedimientos por parte del personal clave.	3	0 - 1: No existe incumplimiento del personal clave 2 - 3: Incumplimiento de políticas y procedimientos por funcionarios claves que no afectan significativamente el proceso 4 - 5: Incumplimiento de varias políticas y procedimientos por funcionarios claves que afectan significativamente el proceso
B. Estructura y Eficacia del Control Interno		
Reportes para el monitoreo de las operaciones	3	
Existencia de reportes para monitorear las operaciones.	3	0 : Existen definidos reportes, procedimientos formales y funcionarios responsables para el monitoreo. 1 -2: Existen reportes, y monitoreo no frecuente y no se han definido procedimientos ni funcionarios responsables. 3 -4: Existen reportes, no se realizan monitoreo y no se han definido funcionarios responsables. 5 : No existen reportes, procedimientos y tampoco se han definido funcionarios responsables.
Apropiados niveles de supervisión y revisión	2,5	
Adecuada segregación de funciones	1	0 : Existe adecuada segregación de funciones. 1 : Algunas actividades que no afectan

Factores de Riesgo	Puntaje del Factor de Riesgo	Explicación de Evaluación
		significativamente el proceso, no tienen una adecuada segregación de funciones 2-3: Gran parte de las actividades que pueden afectar significativamente al proceso no se encuentran segregadas. 4-5: Ausencia total de segregación de funciones.
Evidencia de revisión y supervisión	4	0 : Existe evidencia de supervisión 1 - 2: Existe supervisión pero no existe una adecuada evidencia. 3 - 4 : No existe supervisión y evidencia en procedimientos significativos. 5 : No existe supervisión
Conocimiento y habilidades del personal	2,7	
Personal del área cumple con el perfil requerido para el cargo	2	0 : Personal cumple con el perfil requerido para los diferentes cargos 1 - 3: Personal cumple parcialmente con el perfil requerido para los cargos. 4 - 5: Personal no cumple con el perfil requerido para los cargos asignados.
Experiencia en el desempeño de funciones	3	0 - 1: Desempeño de funciones en el cargo mayor a tres años y demuestra efectividad y eficiencia. 2 - 3: Desempeño entre 1 y 3 años en las funciones y su efectividad y eficiencia están en proceso de afianzamiento. 4 : Desempeño de las funciones o cargos similares hasta un año. 5 : Sin experiencia en el cargo o funciones similares.
Existencia de planes de capacitación	3	0 : El personal ha recibido capacitación formal (interna o externa) con respecto a las políticas y procedimientos, aspectos legales, relacionados con el cargo, en los últimos 12 meses; o, no han existido cambios relevantes

Factores de Riesgo	Puntaje del Factor de Riesgo	Explicación de Evaluación
		en sus funciones. 1 - 3: El personal ha recibido capacitación formal con respecto a sus funciones, en un tiempo mayor a 12 meses. 5 : No existe capacitación ni un plan anual.
Adecuados controles físicos para evitar el acceso a datos, operaciones y áreas restringidas	2	
Controles duales en cajas y bóvedas		0 : Se cumplen con los controles duales. 5: No se cumplen con los controles duales.
Cajas fuertes para custodia de efectivo (procesos relacionados en sucursales)		0 : Existen y se utilizan cajas fuertes 5: No existen o no se utilizan cajas fuertes
Sistema de archivo de documentos relevantes	3	0 : Archivo adecuado de documentación relevante en cajas de seguridad 1 -2 : Sistema de archivo físico no es caja de seguridad, pero brinda salvaguarda adecuada. 3 - 4: Los documentos relevantes se resguardan en un archivador simple sin acceso restringido. 5 : El sistema de archivo no brinda ningún tipo de seguridad.
Controles de acceso a áreas de la Institución, tanto a funcionarios como a personas externas.	2	0 : Existen sistemas automáticos que capturan el ingreso/salida de personas y son efectivos. 1 - 2: El control de acceso se realiza mediante bitácoras manuales y las mismas son validadas por parte de un funcionario independiente en forma periódica. 3 - 4: Existen sistemas automáticos/manuales; sin embargo, no funcionan y/o no cuentan con monitoreo adecuado. 5 : No existen sistemas automáticos ni manuales para el control de acceso.

Factores de Riesgo	Puntaje del Factor de Riesgo	Explicación de Evaluación
Sistemas de seguridad (alarmas, monitoreo de entrada y salida)	1	0 : Existen sistemas de seguridad: alarmas, monitoreo de entrada y salida, cámaras y guardianía (de ser necesario). 1 - 2: Existen sistemas de seguridad: alarmas, monitoreo de entrada y salida, no existen cámaras ni vigilancia armada (guardias). 3 - 4: Los sistemas han presentado deficiencias. 5 : No existen sistemas de seguridad.
Seguridades de los sistemas informáticos	2	Considerar: a. Perfiles de acceso están conforme a funciones b. Presencia de usuarios autorizados. c. Existencia de logs de auditoría (rastro de las transacciones) d. Inexistencia de usuarios genéricos ---------- 0-1 : Cumplimiento de a),b), c), d). 2 : Cumple al menos 3 de los factores 3 : Cumple al menos 2 de los factores. 4 - 5: No cumple ninguno de estos factores.
Grado de implementación de recomendaciones de auditorías anteriores	4	
Observaciones no regularizadas de anteriores auditorías	4	0: Todas las observaciones de Auditorías anteriores fueron implementadas 1: hasta el 5% de observaciones 2: entre 6% y 15% 3: más del 15%. Un punto adicional para observaciones de Riesgo Moderado y dos puntos para las de Riesgo Alto
Reincidencia de las observaciones no regularizadas	4	1: hasta el 5% de observaciones de la presente revisión son reincidentes 2: entre 6% y 15% 3: más del 15%.

Factores de Riesgo	Puntaje del Factor de Riesgo	Explicación de Evaluación
(Se refiere a observaciones que fueron regularizadas pero su incumplimiento se convirtió en recurrente).		Un punto adicional para observaciones de Riesgo Moderado y dos puntos para las de Riesgo Alto.
C. *Calidad e Integridad de la Información Financiera e Información Gerencial.*		
Adecuados sistemas de información gerencial	2,5	
Los sistemas que intervienen en el proceso, emiten reportes gerenciales	3	0 : El sistema emite reportes gerenciales y son utilizados por el personal clave. 1 - 3: El sistema emite reportes gerenciales y no son utilizados por el personal clave 4 - 5: El sistema no emite reportes gerenciales
Emisión de reportes (automáticos y manuales)	2	0 : Todos los reportes son automáticos 1 -2: Los reportes manuales corresponden a un 25% de la información relevante. 3 -4 : Los reportes manuales corresponden hasta un 50% de la información relevante. 5 : Más del 50% de los reportes son manuales.
Integridad de las fuentes de información	3	
Integridad de las bases de datos	3	0: Las bases de datos que intervienen en el proceso, provienen de sistemas cerrados, en los cuales no es posible la manipulación. 5: Las bases de datos que intervienen en el proceso, no provienen de sistemas cerrados y/o es posible la manipulación.
Revisión independiente y conciliación de la información	3	

Factores de Riesgo	Puntaje del Factor de Riesgo	Explicación de Evaluación
Frecuencia de la conciliación de la información	3	0 : Se realiza una conciliación frecuente y oportuna (diaria, semanal, mensual, etc., dependiendo de la naturaleza de cada proceso) 1 - 2: Los reportes se concilian pero presentan diferencias inmateriales. 3 - 4: Se realiza una conciliación de manera esporádica y las diferencias son importantes y no regularizadas 5 : No se realizan conciliaciones de la información.
D. Efectividad de la Gerencia		
Efectividad de la gerencia (monitoreo y control)	3,5	
La gerencia investiga y monitorea continuamente (fuentes internas y externas) sobre los riesgos que afectan a la organización y a su proceso	3	0 : Existe un sistema/procedimiento formal debidamente aprobado para la investigación y monitoreo de riesgos, el cual se aplica sistemáticamente. 1 -2: Existe un sistema/procedimiento formal para la investigación y monitoreo de riesgos, sin embargo su aplicación ha alcanzado máximo un 75% del total del proceso/cuenta. 3 -4 : Existe un sistema/procedimiento formal para la investigación y monitoreo de riesgos, sin embargo es obsoleto o insuficiente para su propósito final. 5 : No existe un sistema de investigación ni monitoreo de riesgos.
La gerencia actualiza los manuales de procedimientos conforme los nuevos requerimientos del proceso (riesgo y controles), en forma oportuna.	4	0 : La actualización de manuales es inmediata, conforme a los cambios del proceso (máximo 30 días). 1 -2: La actualización de manuales es mediata, conforme a los cambios del proceso (máximo 60 días). 3 -4 : La actualización de manuales es tardía, frecuencia mayor a 60 días. 5 : No existe actualización de manuales,

Factores de Riesgo	Puntaje del Factor de Riesgo	Explicación de Evaluación
		conforme los cambios del proceso.
Conocimiento, experiencia y habilidad	2	
Perfil profesional conforme funciones	2	0 : El perfil profesional de la gerencia corresponde con las funciones asignadas 1 - 3: El perfil profesional corresponde parcialmente con los requerimientos del cargo. 4 - 5: El perfil no está de acuerdo con las funciones que desempeña y son totalmente diferentes al perfil del puesto.
Experiencia profesional	2	0 - 1: Experiencia mayor a tres años y demuestra efectividad y eficiencia en el cargo. 2 - 3: Experiencia entre 1 y 3 años en las funciones y su efectividad y eficiencia están en proceso de afianzamiento. 4 : Experiencia profesional hasta un año en las funciones que desempeña o en cargos similares. 5 : Sin experiencia en el cargo o funciones similares.
Adecuada supervisión	2	
Frecuencia y oportunidad de la supervisión	2	0 : Evidencia de supervisión continua y oportuna y seguimiento a instrucciones. 1 - 2: Evidencia de supervisión; sin embargo, las principales decisiones tomadas, no se han implantado en forma oportuna y adecuada. 3 - 4: Supervisión no regular. 5 : No existe supervisión.
Adecuada comunicación de la gerencia	3	

Factores de Riesgo	Puntaje del Factor de Riesgo	Explicación de Evaluación
Comunicación de la información oportuna	3	0 : La transmisión de información relevante es oportuna y por escrito. 1 - 3: La información se comunica en forma verbal y se efectúan comunicaciones por escrito con cierta demora (hasta una semana). 4 - 5: No existe evidencia de transmisión de información y decisiones relevantes.
Uso de reportes gerenciales para medir y monitorear	3,7	
Utilización de reportes que faciliten el monitoreo de las operaciones y el cumplimiento de los controles implantados.	3	0 : Utilizan reportes únicamente automatizados para el monitoreo y supervisión de las operaciones; adicionalmente, éstos arrojan alertas a través de la cuales se pueden implementar mejores controles. 1 - 2: Utilizan reportes manuales y automatizados para el monitoreo y supervisión de las operaciones. 3 - 4: No se han incluido en el sistema de reportes todos los informes necesarios para toma de decisiones. 5 : No utilizan reportes para el monitoreo de las operaciones.
Utilización de presupuestos para evaluación	3	0 : Se realizan evaluaciones mensuales del presupuesto. 1 - 2: Las evaluaciones presupuestarias se efectúan por períodos mayores a un mes (hasta 3 meses). 3 - 4: El análisis presupuestario se realiza en forma esporádica (mayor a 3 meses). 5 : El área no realiza evaluaciones periódicas del presupuesto o no existe presupuesto.
Existencia de comités o juntas. Se emiten actas donde se resumen las principales decisiones.	5	0 : Existen actas de los comités donde se incluyen las decisiones tomadas y éstas se encuentren debidamente foliadas, enumeradas y con las firmas respectivas y archivadas adecuadamente.

Factores de Riesgo	Puntaje del Factor de Riesgo	Explicación de Evaluación
		1 - 3: Las actas se oficializan vía e-mail entre los asistentes a los comités, sin embargo, no se mantiene un control del archivo (electrónico o físico) de dichas comunicaciones. 4 - 5: Los comités no formalizan las decisiones mediante actas o algún documento similar.

Tabla 16:

Matriz Detallada de Factores de Riesgo – Proceso 2 (Corresponsales No Bancarios)

Factores de Riesgo	Puntaje del Factor de Riesgo	Ponderación de Riesgo	Riesgo ponderado calculado
FACTORES DE RIESGO INHERENTE			
A. Complejidad y tamaño de la Operación			
Complejidad de la Operación	5	40%	2
Grado de automatización	3,7	30%	1,1
Registro contable de las operaciones	4	30%	1,2
Subtotal		100%	4,3
B. Naturaleza del Entorno de Negocios			
Complejidad de leyes y regulaciones.	2	60%	1,2
Historia de pérdidas por fraude y errores externos	2	40%	0,8
Subtotal		100%	2
C. Naturaleza Interna de la Entidad			
Historia de pérdidas por fraude y errores internos	4,50	40%	1,8

Rotación de Personal	4,33	30%	1,3
Comisiones del personal	5,00	30%	1,5
Subtotal		100%	4,6
TOTAL RATIO DE RIESGO INHERENTE		**Moderado**	**11**
FACTORES DE RIESGO DE CONTROL			
A. Cumplimiento de políticas, procedimientos y normativa legal			
Diseño e implementación de políticas y procedimientos	4	25%	1
Adecuadas y claros niveles de autorización	3	25%	0,75
Cumplimiento de leyes y reglamentos relevantes por parte del personal clave	1	25%	0,25
Nivel de cumplimiento con políticas y procedimientos relevantes.	3	25%	0,75
Subtotal		100%	2,75
B. Estructura y Eficacia del Control Interno			
Reportes para el monitoreo de las operaciones	3	20%	0,6
Apropiados niveles de supervisión y revisión	2,5	20%	0,5
Conocimiento y habilidades del personal	2,7	20%	0,5
Adecuados controles físicos para evitar el acceso a datos, operaciones y áreas restringidas	2	20%	0,4
Grado de implementación de recomendaciones de auditorías anteriores	4	20%	0,8
Subtotal		100%	2,8
C. *Calidad e Integridad de la Información Financiera e Información Gerencial.*			
Adecuados sistemas de información gerencial	2,5	30%	0,75
Integridad de las fuentes de información	3	30%	0,9

Revisión independiente y conciliación de la información	3	40%	1,2
Subtotal		100%	2,85
D. Efectividad de la Gerencia			
Efectividad de la gerencia (monitoreo y control)	3,5	20%	0,7
Conocimiento, experiencia y habilidad	2	20%	0,4
Adecuada supervisión	2	20%	0,4
Adecuada comunicación de la gerencia	3	20%	0,6
Uso de reportes gerenciales para medir y monitorear	3,7	20%	0,7
Subtotal		100%	2,8
TOTAL RATIO DE RIESGO DE CONTROL		**Bajo**	**11,27**
TOTAL RATIO DE RIESGO AGREGADO		**Alto**	**22,17**

Resultado: En la evaluación del proceso de Corresponsales No Bancarios podemos concluir que este proceso mantiene un riesgo inherente moderado; siendo el factor de riesgo más relevante de la complejidad y tamaño de la operación; y, naturaleza interna de la entidad. Adicionalmente, este proceso mantiene un riesgo de control bajo, lo cual indica que sus controles son débiles o en algunos casos no existen, los factores de riesgo donde se debe poner mayores controles es la eficacia y estructura del control interno y calidad e integridad de la información financiera y gerencial. Concluyendo este proceso es de Riesgo Alto con un ratio de 22 puntos.

3.2.7. Matriz de calificación del universo de procesos

Una vez diseñada la matriz de factores de riesgo, se debe calificar los procesos que forman parte del Universo Auditable conforme la Matriz, en función de la calificación obtenida se

debe determinar los ciclos de revisión: Riesgo Alto se debe revisar cada año, los procesos con riesgo Moderado cada dos años y los procesos con riesgo Bajo cada tres años.

La matriz de riesgo no puede ser modificada, ni forzada para sustentar la inclusión o exclusión de revisiones que deben ser realizadas en el plan anual de auditoría. Si la revisión del proceso/cuenta, es un requerimiento legal, regulatorio o sensible, se considera que debe ser incluido todos los años en el plan de rotación, de igual forma debe realizarse el análisis de sus factores de riesgo por medio de esta matriz.
Posterior a la calificación de todos los procesos, se procede a elaborar la siguiente matriz donde se visualiza la priorización de las revisiones:

Tabla 17:
Matriz de calificación del universo de procesos

Procesos	Riesgo			Calificación	Definición del Plan		
	Inherente	Control	Total		Año 1	Año 2	Año 3
Transporte de Valores	8,17	7,37	15,54	Moderado	X		X
CNB's	11	11,27	22,27	Alto	X	X	X
Proceso XXXXX				Bajo			X

3.2.8. Definir el Plan de Auditoría Interna

Finalmente la definición de los procesos a ser auditados y los ciclos de auditoría respectivos comprenden el eje del Plan de Auditoría, posteriormente se debe realizar la estimación y asignación de recursos (equipo de auditores, horas de auditoría, cronograma general) y proceder a la ejecución del plan.

El plan de auditoría basada en riesgos debe ser actualizado anualmente, salvo circunstancias especiales o extraordinarias o por normativa legal, existe excepciones en los cuales debe actualizarse más frecuentemente (por ejemplo, trimestralmente), en respuesta a los cambios del negocio de la entidad, operaciones, programas, sistemas y controles de la

Institución Financiera, por ello este plan debe ser igual que el ambiente de negocios, debe ser dinámico y debe reflejar cambios de acuerdo al entorno del perfil de riesgos de la organización. Si se identifican cambios de debe revalidar el plan con el comité, la dirección y la gerencia de la entidad. Se debe revaluar el plan periódicamente, por lo menos una vez al año para tomar en cuenta cambios críticos y evitar re elaborar un plan anual.

El plan de Auditoría debe ser conocido y aprobado por el Comité de Auditoría y Directorio General de la Institución, para que a su vez ellos conozcan de mejor manera y se comprometan más con la identificación de los riesgos dela organización, y a su vez se pueda mejorar significativamente las expectativas del Comité a través de la ejecución del plan de auditoría.

El Plan de Auditoría, debe ser preparado y presentado en un documento formal, incluyendo lo siguiente:

- Carátula
- Índice
- Introducción
- Entendimiento del modelo de negocio de la Institución Financiera
- Estrategia Institucional
- Estructura organizacional
- Principales funciones y responsabilidades de la Administración
- Visión, Misión de Auditoría Interna
- Metodología de Auditoría
- Objetivos de la Auditoría
- Organigrama de Auditoría
- Requerimientos de recursos materiales y económicos
- Estrategia de Personal
- Cronograma de Plan de Auditoría: Aseguramiento y Consultorías (De acuerdo a la circular No. INIF-DRN-2003-21
- Informes a emitir

4. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

La investigación realizada permitió cumplir con los objetivos propuestos y establecer las siguientes conclusiones:

1. Todas las organizaciones enfrentan cada vez mayor grado de incertidumbre, por efectos de la globalización, la complejidad de los negocios y los avances tecnológicos, el desafío es determinar cuánto de esta incertidumbre se debe estar preparados para aceptar. Con la evolución y dinámica de los negocios se plantea una gran oportunidad para fortalecer y optimizar el control interno en el sentido de agregar valor y contribuir efectivamente al logro de los objetivos de las Instituciones.

   Siendo el control interno una combinación de reglas, principios, o medidas enlazadas entre sí desarrolladas dentro de una organización para garantizar su estructura, con la finalidad de lograr la protección del patrimonio, con el adecuado cumplimiento de políticas y procedimientos; es muy adecuada la aplicabilidad del sistema COSO dentro de las Instituciones Financieras, sin embargo, hoy en día es más apropiado fortalecer este control interno en base a la identificación y gestión de los riesgos aplicando el COSO ERM, ya que se involucra dentro de la empresa como una cultura de enfoque de riesgos y una herramienta de gestión que permite identificar y controlar los riesgos (financieros, operativos y estratégicos) y ayuda a implementar oportunamente acciones preventivas y correctivas, y prever las consecuencias potenciales de eventos futuros.

2. La institución financiera no dispone de una metodología que contenga lineamientos claros de cómo realizar una auditoría basada en riesgos y que sirva de marco de referencia para ejecutar sus funciones, la misma es realizada en base a procedimientos muy generales, criterio de los auditores e información histórica que

sustente en parte lo exigido por el organismo de control que es orientado a la evaluación de los riesgos del negocio y hacia una actividad de asesoría, que mediante la aplicación de estándares de alta calidad y sin afectar su independencia y juicio crítico, contribuya de mejor manera a la optimización de los procesos del negocio y a la minimización de los riesgos, identificando situaciones de mejora y formulando recomendaciones de valor agregado.

3. Según la evaluación realizada al área de Auditoría Interna de la Institución Financiera, se validó que, al realizar el plan anual para el desarrollo de las auditorías, por no contar con una metodología establecida y definida, es realizada sin una profundización de la alineación de los objetivos estratégicos de auditoria con los de la organización. Adicionalmente, no se valida si todos los procesos que auditoría toma en cuenta para la planificación son los que mantiene la institución, por lo cual existe la probabilidad de dejar procesos relevantes fuera de las revisiones anuales que, al no identificar oportunamente errores, irregularidades, debilidades de control, pueden desencadenar en posibles fraudes internos y externos, multas y sanciones por los entes de control e incluso el cierre de la entidad.

4. Uno de los factores importantes para que no se esté aplicando una metodología es que, todo el personal no esté involucrado en los cambios y enfoques que da el COSO ERM, debiéndose, principalmente, a que no se ha impartido capacitación adecuada y periódica del nuevo enfoque de la auditoria basada en gestión de riesgos, lo que provoca que no se mantenga una directriz clara de cómo ejecutar su trabajo, identificando dentro de los procesos áreas o actividades críticas, ya que la función de la Auditoria, hoy en día, es preventiva antes que correctiva.

4.2. Recomendaciones

Las recomendaciones que se han establecido al concluir esta investigación, son las siguientes:

1. Para mantener una certeza razonable en la consecución de los negocios de la Institución Financiera y enfrentarnos al desafío de un mundo cambiante, es necesario implementar en la organización, adecuadas metodologías de control interno, debido a las exigencias actuales se debe enfocar y profundizar una gestión de riesgos en todos las áreas de la empresa, por ello es adecuado y recomendable aplicar una metodología basada en riesgos, que de acuerdo a la presente investigación es aplicable en la organización el COSO ERM, tomándolo como marco de referencia para el desarrollo de una Auditoria Basada en Riesgos, ya que ayudará a atacar a los factores más críticos que impiden la consecución de objetivos y estrategias institucionales.

2. Se recomienda que la Institución Financiera aplique la metodología de Auditoría Basada en Riesgos diseñada para el área de Auditoría Interna, como base fundamental para fomentar una cultura organizacional que involucra una actitud de cambio del personal y un real compromiso en sus actividades. Este enfoque apoyará al desarrollo de las funciones del área de auditoría interna de la entidad y que su planificación, bajo la metodología planteada, conduzca a abarcar el universo de procesos y cómo estos se relacionan con las estrategias / objetivos de la institución y a evaluarlos en base a una Matriz de Factores de Riesgo, la cual permitirá al Auditor Interno planificar de una manera más eficiente en función de los procesos más críticos o los que requieren mayor atención debido a la susceptibilidad y debilidades.

3. Según la presente investigación y su aplicación en la Institución Financiera evaluada se determinó que es necesario destacar que, dentro de la aplicación de la Metodología ABR, se debe profundizar y aplicar una adecuada alineación de los objetivos estratégicos del Área de Auditoría Interna con los objetivos macro de la Institución y así actuar en conjunto con la consecución del logro de estos objetivos, aplicando las estrategias definidas. Adicionalmente, se debe validar tanto los procesos levantados por la organización, como los procesos que se auditan anualmente para relacionarlos e identificar los procesos no tomados en cuenta y así

destacar posibles procesos importantes que no han sido revisados. Con la aplicación de la matriz de factores de riesgo, aparte de brindar una visión clara y precisa de cuáles son los procesos que deben ser revisados de acuerdo a la periodicidad definida (1, 2 o 3 años), se puede destacar en qué áreas o actividades específicas de los procesos evaluados se tiene más falencias, debilidades, ausencias de controles y hasta ser propensos a fraudes internos y externos y así poder aplicar a tiempo medidas correctivas. Parte de la aplicación de esta metodología es dar a conocer el Plan de Auditoría a la administración y la alta gerencia de la institución, representados por el Comité de Auditoría y así involucrarlos en el desarrollo y consecución del plan anual de Auditoría Interna.

4. Adicionalmente, se debe aplicar como política del área de Auditoría capacitaciones periódicas en temas relacionados con el COSO ERM para que puedan ser parte de lo que conlleva un cambio y aplicación de la gestión de riesgos en la ejecución de sus funciones y en el desarrollo de una adecuada planificación anual.

Bibliografía

Auditoría, B. (2009). *Coso I y Coso II.* Recuperado el 2014, de blogauditoria.files.wordpress.com/2009/11/coso_i_y_coso_ii_1_1.ppt

Badillo, J. (Julio de 2010). Auditoría Basada en Riesgos- ABR: Fundamentos y Aplicación Práctica.pdf. Quito, Pichincha, Ecuador.

Banco Central del Ecuador. (2014). Sector Real. *Estadísticas Macroeconómicas, Presentación countural*, 15.

Berbia, P. (2008). *Evaluación Eficaz del Sistema de Control Interno.* Florida: The Institute of Internal Auditors Research Foundation (IIARF).

Díaz, J. (2013). Qué es la cultura organizacional de una empresa.

ElPrisma.com. (s.f.). *El prisma.com.* Recuperado el 2014, de El prisma.com: http://www.elprisma.com/apuntes/administracion_de_empresas/control/

Ernst&Young. (2010). Los primeros 10 Riesgos para los Negocios.

España, I. d. (2011). *Marco Internacional para Práctica Profesional de la Auditoría Interna.* Madrid: Insttituto de Auditores Internos de Ecuador.

Estupiñán Gaitán, R. (2006). *Administración de Riesgos E.R.M y la Auditoría Interna.* Bogotá: Ecoe Ediciones.

Financiera, I., & Riesgos. (2014).

Geovanni Basabe, M. B. (2013). Cultura organizativa: análisis de su relación con la estrategia y gestión empresarial. Quito, Pichincha, Ecuador: UTE.

Instituto de Auditores Internos. (s.f.). Auditoría Interna: Servicios de aseguramiento y consultoría. I.A.I.

Instituto de Auditores Internos. (s.f.). *Rol del Auditor Interno en el ERM.pdf*. Recuperado el 2014, de www.theiia.org

Internos, C. &. (1997). *Los nuevos conceptos del control interno (Informe COSO).* Madrid: Ediciones Dïaz de Santos S.A.

Kopelman, A., B., & R., G. (1990). *The role of climate and culture in productivity.* En Schneider, B 1990 Obv Cit. pp 282-318.

Lefcovich, M. L. (s.f.). *Auditoría Interna. Un enfoque sistémico y de mejora contínua. Monografías.com*. Obtenido de : http://www.monografias.com/trabajos15/auditoria-interna/auditoria-interna.shtml#ixzz35VUWLI8o

Mantilla, S., & Cante, S. (2005). *Auditoría del Control Interno.* Bogotá: Ecoe Ediciones.

Mapadeprocesos.pdf. (s.f.). *El Mapa de Procesos y Análisis.* Recuperado el 2014, de http://www.formatoedu.com/web_gades/docs/2__Mapa_de_Procesos_1.pdf

Mautz, R. (1970). *"Fundamentos de Auditoría".* Buenos Aires: Ediciones Macchi.

Monografias.com. (s.f.). *Monografías.com.* Recuperado el 2014, de http://www.monografias.com/trabajos6/nute/nute.shtml#ixzz3AnFdbwpb

Real Academia Española. (2013). *Diccionario de la lengua española*. Obtenido de http://lema.rae.es/drae/?val=metrolog%C3%ADa

SAS 1, A. s. (1972). *Statement on Auditing Standard,*. EEUU: AICPA.

Superintendencia de Bancos y Seguros de la República del Ecuador. (2005). LIBRO I, Normas Generales Para La Aplicación De La Ley General De Instituciones Del Sistema Financiero. *Titulo X.- De La Gestión Y Administración De Riesgos*. Quito: http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/nueva_codificacion/todos/L1_X_cap_V.pdf.

Taller de Producción de mensajes. (s.f.). Recuperado el 2014, de www.perio.unlp.edu.ar/tpm

Wikipedia, E. (s.f.). *http://es.wikipedia.org/wiki/Riesgo.* Obtenido de Wikipedia.

WordPress. (2004). *Definición.de.* Obtenido de Definición.de: http://definicion.de/riesgo/

Yánez, V. E. (2014). *Futuro de la Auditoría Interna.* I.A.I.